A Product of DIGINFO®

Volume 7 I 2023

CYBER MAGAZINE

DG MAGAZINE

The Ultimate Source of Cyber World

PROFILING HACKERS

A CASE OF DANGEROUS JOURNALISM

LEFT OPEN SCADA NETWORKS
SEAMLESS EAVESDROPPING BY CRIMINALS

Cyber Security Conferences
MUST-ATTEND LIST FOR 2023

PHISHING ATTACKS
DEEP DOWN EXPLANATION AND DEFENSE STRATEGY

Global Count of Ransomware Attacks
269 IN DECEMBER 2022 ALONE

dgmagazine.diginfo.net

CONTENTS

FROM THE EDITOR

Muhammad Saeed
Chief Editor

New year has already arrived. Contrary to popular notions of celebrating, we feel that such occasions should be spent on introspection. We have done just that by selecting news and stories that cast a critical eye on the times that are gone, knowing well that the past is full of stories and events that provide lessons to learn.

In choosing topics for research-based articles, we have taken care to provide interesting and entertaining material. Of course, the permanent value and enduring importance are the qualities that remain constant. The lead story, though lengthy, is replete with interesting anecdotes and draws inspiration from classical crime stories. Hacker Profiling may seem a relatively new subject but its genesis is rooted in the age-old methods of detective work.

The other articles are at par with the lead story highlighting the fact that cybersecurity has become an indispensable part of our daily lives. It has come to permeate our day to day affairs with the intensity that no one could have imagined a few years before now.

So keep reading. And keep on referring the material to your fellow professionals. A good thing must be shared. And reading material is not just good, it is excellent stuff.

EDITORIAL BOARD

Muhammad Saeed

Head of Editorial Board

Muhammad Saeed packs a lot more energy in his frame than anyone can guess. His biographical data reads like some stuff of dreams. Apparently he imagines something and goes out to get it without fail.

His academic record, to say the least, is impressive. A bachelor's from University of Karachi, a master's from LUMS and a doctorate from University of Karachi. As if that was not enough, he has also done some technical courses from prestigious institutions.

Now, as assistant professor at the same university he earned his doctoral degree from, he has carved a life steeped in erudition and academic pursuits. Already, he has authored or co-authored several research papers on subjects related to Computer Science or Information Technology. It is not surprising that quite a few of his students have demonstrated their creative talent under his tutelage.

Saeed is a restless soul. He is not the conventional 'sit back, relax and enjoy' type of person. He prefers to go out and discover what is there that can interest him. Inquisitiveness and enquiry mark his professional ethics. As a routine, therefore, he ventures out to participate in workshops, conferences and research studies, often on esoteric subjects.

Our country needs people of his type. Go-getters who define their goals and the path that takes them right there. In no time.

EDITORIAL BOARD

Dr. Ashfaq Malik
Member Editorial Board

He spent a lifetime in the strictures of the military environment. So, it was natural of him to become a disciplinarian that he is. The fact is evident from a list of educational accomplishments and work experiences that goes beyond the ordinary.

His first taste of victory within the military culture came in the early 90s when he graduated from Pakistan Naval Academy, which earned him a commission in Pakistan Navy as Naval Officer. That marked the beginning of his professional career. During his duty, he took up studies to graduate as an Electrical Engineer and then penned a doctoral thesis related to Electrical Engineering with specialization in Networks and Information Security.

He has a rich work experience that spans at least 25 years. During this time, he performed a variety of teaching and managerial duties at Pakistan Navy, National University of Sciences and Technology (NUST) and affiliated institutes of Sindh Board of Technical Education (SBTE). He has taken early retirement from the Navy to concentrate full time on research and teaching. At the time of leaving the services, he was working as a commander.

His knowledge and deep understanding of cyber security issues makes him an asset for DIGINFO, a company that has set top standards for itself.

In recognition of his illustrious career, both as an educationist as well as an administrator of top order, Dr Ashfaq was twice recommended for the prestigious Tamgha-e-Imtiaz. This alone speaks a lot about the singular dedication and extraordinary passion personified by him.

We desperately need such people. That he is in our midst is a privilege and an honour for all.

Shahzad Saleem
Member Editorial Board

He is an Assistant Professor at College of Computer Science and Engineering, University of Jeddah, KSA.

He also serves as head of the Department of Information Security, KTH-AIS Lab, School of Electrical Engineering and Computer Science, NUST, the top university of Pakistan.

He has over fourteen years of teaching, research and industry experience in various executive positions. He has been involved in more than twenty research publications indexed by Scopus, ISI and HEC. Right now, he is co-authoring a research proposal of US$400,000 under Pak-China Reseach Grant. The areas of research that interest him include Digital Forensics, Authentication and Access Controls.

His teaching experience touches on subjects like Digital Forensics, Computer Forensics, Network Security, Cryptography, Computer Security, Introduction to Algorithms and Data Structures. And there is a variety of other areas he is actively involved in which makes his portfolio rich and versatile. In his capasity as an Editorial Board member and with his valuable counsel, he is bound to make his presence felt at DG Magazine.

EDITORIAL BOARD

Adnan Masood
Member Editorial Board

He is an Artificial Intelligence and Machine Learning researcher, software architect and Microsoft MVP (Most Valuable Professional) for Artificial Intelligence. As Chief Architect of AI and Machine Learning, at UST Global, he collaborates with Stanford Artificial Intelligence Lab, and MIT AI Lab for building enterprise solutions. He has authored "Functional Programming with F#" which rose to become an Amazon bestseller in programming languages.

Dr. Masood teaches Data Science at Park University and Windows Communication Foundation (WCF) courses at the University of California, San Diego. He is a regular speaker to various academic and technology conferences, local code camps, and user groups. He also volunteers as STEM (Science Technology, Engineering and Math) robotics coach for elementary and middle school students.

Dr. Masood is a strong believer in community service. He co-founded and presides Pasadena .NET Developers group. He also organizes Tampa Bay Data Science Group, and Irvine Programmer meet-up. His recent talk at Women in Technology Conference (WICT) Denver highlighted the importance of diversity in STEM and technology areas, and was featured in press and on news channels.

His presence on the editorial board of DG Magazine means an assurance of quality content and up-to-date information.

Irfan Nabi
Member Editorial Board

He is a researcher, teacher and administrator all rolled into one healthy mind. In pursuit of his interests, he has gone to places far and wide and worked hard to reach milestones that others only dream about.

Dr. Irfan's ascension to a position of esteem and enlightenment began with a basic degree in Electrical Engineering from NWFP University of Engineering & Technology, Peshawar, Pakistan. Later on he earned a doctorate in Management Information Systems from Institute of Business Administration, Karachi. This institute is also the place where he works as Academic Director, Project Management Program. The position offers him a slew of opportunities to conduct research and provide guidance to the students. Dr. Irfan has contributed his research articles to various publications, journals and conferences. He also finds time to play an active community service role in and around his neighborhood.

It is easy to surmise that his knowledge and experience would go far in raising the standards of our magazine. More important, his counsel would be a great help in maintaining those standards.

CREDENTIALS

EDITORIAL

PRINCIPAL & FEATURE WRITER
Hamed Mohiuddin

ARTICLES RESEARCHER
Salman Khan

SENIOR RESEARCHER & NEWS WRITER
Okasha Mussa Sujela

CYBER RESEARCHER & COORDINATOR
Omer Imran

MANAGEMENT

DIRECTOR OF CYBER TECHNOLOGY
Muhammad Saleem

CONCEPT DIRECTION & STRATEGY PLANNING
Furqan Mirza

MARKETING & BUSINESS DEVELOPMENT
Akmal Khan

ART DIRECTION & DESIGN
Imran J

DG MAGAZINE is an initiative of DIGINFO Group aimed at creating awareness about cybersecurity. The publication is distributed in a variety of ways: electronically via mail, HTML, pdf, mobile message and online flipbook.

PRESIDENT
Muhammad Saleem

V.P. INTERNATIONAL
Muhammad Saeed

COO & STRATEGY
Furqan Mirza

Lead Graphic Designer / Creative Strategy
Quratul Ain Khalid

MEDIA & PUBLISHING
Entity of **DIGINFO Group**
info@diginfo.net

CYBER AWARENESS

In our country, people woke up to the dangers of cyber attacks when most others were at war and devising strategies to fight the scourge. Only recently, several hacking attacks on large businesses culminated in huge ransom demands. These attacks caught everyone unawares and caused tremendous financial losses together with bruised reputation.

Such incidents have highlighted the importance of cybersecurity and the issues surrounding it.

The pressure from the hackers is mounting and they have the power to put lives in turmoil. Anyone who is not aware of the fact is living dangerously.

The best strategy is to be aware and take proper safety measures.

PROFILING HACKERS

A CASE OF DANGEROUS JOURNALISM

The term 'criminal profiling' gained wider recognition soon after the publication of retired FBI agent John Douglas's seminal book 'Headhunter—Inside the FBI's Elite Serial Crime Unit.' John Douglas, during his extensive career at the FBI Behavioral Analysis Unit, devised new methods for apprehending serial killers and other violent offenders. The character of John Crawford in the 1991 thriller 'Silence of the Lambs' is purported to be based on his work as the head of FBI's Elite Serial Crime Unit. 'Criminal Profiling' helps investigators make educated guesses about the perpetrators of such heinous deeds.

After retiring from his service, where he remained overworked, John Douglas turned to writing, appearing on television talk shows and attending online events as guest speaker. He has written many books which are a mix of psychology, pattern recognition and inductive/deductive reasoning. He says, "To understand the artist, you must look at the artwork…to understand the criminal, you must look at and study the crime itself." According to an announcement of an online event where Douglas was a speaker, "Douglas' ability to link behavior and evidence makes him the lawman serial killers fear."

The activity we call 'Hackers' Profiling' draws inspiration from the works of Douglas and it is based on the idea that criminals, after committing evil, leave their footprints behind. There are telltale signs of who might have done the job. Every crime carries a signature of the person who did it. The investigators try to recognize the patterns and peculiar signs which may lead to the criminal.

GLIMPSES FROM HISTORY.
The earliest example of 'Criminal Profiling' dates back to the Victorian era of late nineteenth century. In 1888, five women were killed and their bodies mutilated by a still unknown serial killer known as Jack the Ripper. The last of his victims was Mary Jane Kelly whose body was discovered in a small room of Dorset Street, East End of London.

Dr Thomas Bond, professor of forensic medicine, was asked to comment on the earlier murders of the Ripper. While he was still studying the documents to comment on, another murder took place and Dr Bond was called upon to carry out the autopsy. He examined the badly mutilated corpse to offer his own interpretation of the behavior of the murderer. In the report, Dr Bond wrote:

"All five murders were no doubt committed by the same hand. In the first four the throats appear to have been cut from left to right. In the last case owing to the extensive mutilation it is impossible to say in what direction the fatal cut was made, but arterial blood was found on the wall in splashes close to where the woman's head must have been lying.

"The murderer must have been a man of physical strength and of great coolness and daring. There is no evidence that he had an accomplice. He must in my opinion be a man subject to periodical attacks of homicidal …. mania… It is of course possible that the homicidal impulse may have developed from a revengeful or brooding condition of the mind, or that Religious Mania may have been the original disease, but I do not think either hypothesis is likely. The murderer in external appearance is quite likely to be a quiet inoffensive looking man probably middle-aged and neatly and respectably dressed. I think he must be in the habit of wearing a cloak or overcoat or he could hardly have escaped notice in the streets if the blood on his hands or clothes were visible.

"Assuming the murderer to be such a person as I have just described he would probably be solitary and eccentric in his habits, also he is most likely to be a man without regular occupation, but with some small income or pension. He is possibly living among respectable persons who have some knowledge of his character and habits and who may have grounds for suspicion that he is not quite right in his mind at times. Such persons would probably be unwilling to communicate suspicions to the Police for fear of trouble or notoriety, whereas if there were a prospect of reward it might overcome their scruples."

Dr Bond's original work is a huge influence on professionals to this day. Detectives investigating violent crimes often employed the methods invented by Dr Bond. That is why he is considered as the first 'offender profiler.'

But there was a hiatus of nearly seven decades to bring about any remarkable progress in the investigative process. In 1970, FBI agents Howard Teten and Patrick Mullany started up criminal profile program which was named as Applied Criminology. This led to the formation of Behavioral Science Unit as a permanent department of FBI. A lot of development followed when Robert Ressler, John Douglas and Ann Burgess started interviewing serial killers to find out how the mind of a criminal works and how it has a close connection with the crime itself. Their work received wide recognition and, as a result, the idea that the crime and the way it was perpetrated may provide clues to the personality of the person who committed the deed gained wide recognition.

Employing the techniques that they had developed for years, John Douglas and his team were able to predict about the serial killer's personality and the social background by thoroughly examining the crime scene. In most cases their predictions turned out to be accurate to a great degree. In one such case, law enforcement agents were alarmed to see that kids aged 7 to 12 kept disappearing in an African American neighbourhood. The bodies that were discovered pointed to the fact that the job was done by a single hand. By examining the crime scene and other factors, John Douglas and his team predicted that the serial killer is a young black male with a German shepherd. Sure enough, a black 23 year old male was apprehended soon afterward who had a pet German shepherd. The prediction made by the Douglas team was stunning. And it proved that the methods they were employing were fairly accurate. Douglas's contribution in getting to the Unabomber is also well documented.

APPLYING THE TECHNIQUES TO HACKERS.

Criminal profiling techniques were found to be useful in solving crimes of violent nature: homicide, rape, arson, bombing, and other similar ones. Hacking and hackers were not considered to be preferred for profiling techniques. Still one factor is common to both natures of crime. Criminals who commit violent crimes are usually prone to repeat their deeds over and over again. It is a psychological condition.

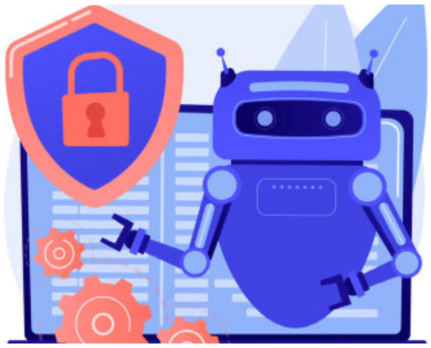
To fully understand computer attacks, two professionals can provide valuable information to start the investigation. Computer security experts can answer questions like 'What has happened?' and 'How did it happen?' The criminal profiler can answer questions like 'Why the attack took place?' and 'Who launched the attack?'

The answers to the 'What' and 'How' of a case are obtained by crime scene analysis. In the case of computer crimes, the crime scene isn't a physical place or a geographical entity, but an electronic approximation to fingerprints or DNA traces left behind by the perpetrator: the log files and audit trail of the computer system.

The trained eye of the criminologist is interested in two aspects which are common to hacking incidents and violent crimes. The 'modus operandi' represents the criminal's behavior while committing the crime. This behavior is ever-changing as the perpetrator learns and evolves techniques for committing the deed.

The other aspect is 'signature' which is something invariable. It is like a stamp which the criminal places each time he commits the deed. It is not a necessary feature but it is repetitive.

Hackers indulge in the same practice. They target victims and conduct their operation in a routine fashion creating a pattern which helps investigators to guess who might be behind the act. Profiling saves time by reducing the number of suspects. Investigators—or ethical hackers—get to know where to look for and catch the criminal if a hacker's profile is there as a help.



The hackers' profiler analyzes digital footprints left behind by the criminals. While analyzing the investigators try to answer certain probing questions like 'What might be the goal of the attacker?' or 'Why the attacker was interested in launching that kind of attack?'

To answer such enquiries in a systematic way, The Hackers Profiling Project (HPP) was started in 2004 at UNICRI. The team at HPP was able to identify nine types of attackers.

Wannabe (Lamer). The "wannabe," or a "lamer," is usually a novice who aspires to be a hacker. This breed of trouble makers uses hacker software easily downloadable for free from the internet. And then they post the stuff at random in the shape of messages in large amounts. Since such would-be criminals are not experienced, they act in an amateurish manner and often cause huge damages to computer systems or networks.

Script kiddie. The "script kid" is a hacker who relies on UNIX/Linux scripts written by others. This kind of hacker is only interested in the result and not the coding that delivers the desired actions. Script kiddies lack the technical sophistication to understand how the software works. Perhaps for this reason, they are they are known as "point-and-clickers," and the attacks they launch are referred to as "point-and-click attacks." A 14-year old boy, Mafia Boy, is a well-known example of Script Kiddie.

Cracker. Contrary to the above two, these operators are technically skilled which enable them to achieve their goals. The term "cracker" is now outdated. It was used for those who routinely attempted to break into computer system with malicious intent. Their goal was to gain some profit or to get a kick out of the challenge inherent in this type of work. The Internet Users' Glossary defined a computer cracker as "an individual who attempts to access computer systems without authorization. These individuals are often malicious and have many means at their disposal for breaking into a system."

This term should not be confused with the 'software cracker' which is used for those who crack software protection for illegal reproduction.

Ethical Hacker. This term is reserved for those creative individuals who are fairly skilled in their trade. They are not copycats, rather, they prefer to use their own program. Their sole intent is to serve their community by digging into systems and IT infrastructures, and clearing them of bugs and errors. Ethical hackers are highly sophisticated and are adept at different operating systems. Their skill set can range from Sun Solaris, HP/UX or OpenVMS to Microsoft Windows. Their modus operandi is to launch attacks manually instead of an automated method.

QPS (Quiet, Paranoid, Skilled Hacker). These types of hackers are similar to ethical hackers in many ways. They are creative individuals with an inclination to use their own designed software instead of those made by others.

However, their distinctive character is to immediately disappear from the scene when there is a fear of being caught. They are into this business of attacking IT systems not because of acquiring information; their aim is the pleasure they derive from "that particular release of HP/UX that one is running, or an SS7 backbone.

Cyber-warrior/Mercenary. This breed of miscreants is a relatively new phenomenon resulting from internet's globalization and hacktivism. The mercenary hacker works on commission, and receives handful of money to attack specific targets. Their skill may range from basic to advanced with the ability to launch attacks such as DDoS, Web Defacing or Wi-Fi. Most Russian rogue elements belong to this group of hackers. RBN, the Russian Business Network thrive on the skills of mercenary hacker to advance their agenda of illegal activities.

Industrial Spy Hacker. Industrial espionage has been around since antiquity. Spies often infiltrated the industries and walked out with piles of stolen information stored on floppy disks, cd-roms, microfilms and paper files. Nowadays, there is an addition of USBs and emails for information storage.

Some of the recent incidents of industrial espionage involved active participation of Industrial Spy Hackers. This is a modern approach to the older version of industrial espionage.

Government Agent Hacker. Warfare on global scale has given rise to state-sponsored attacks. Governements, with an intent to consolidate power or exert hegemony, launch attacks on other soils taking help and employing Governement Agent Hackers. This breed of hackers is very skilled and possesses know-how of international markets and how they operate.

Military Hacker. When the HPP research team talked about the existence of such an individual, many analysts raised their eyebrows. But the chain of events leading up to the current situation has confirmed that the reality cannot be denied.

DANGEROUS LIAISONS. The reason cybersecurity has risen to such a significant aspect of corporate culture is that unscrupulous elements have grown in epidemic proportions. Big money and easy money are the key motivators that attract an army of hackers to launch attacks.

When big money is involved, cut-throat competition is bound to make its presence felt. That has happened in the cyber world. Where money was involved, violence went hand in hand. Anyone who tried to stop their run was met with vicious reaction.

Reporters who went after the crime and the criminals remain in great danger. The community of hackers, whose skills generate huge amounts of money, will not remain spectators. They will react and they will react with impunity.

Journalists reporting the crime or profiling the hackers and pinpointing their identity are destined to face the wrath. That is what is happening all over the world. Journalists are being tortured and killed violently for crossing the path of hackers. Those reporting cyber crime and profiling hackers are now embroiled in a battle which is not only dangerous but deadly dangerous.

Security Threats Worldwide in 2022

LOOKING BACK IN TIME TO MOVE FORWARD

In an increasingly polarized world, accusations and counter accusations are the norm. China, Russia, Iran and North Korea form a bloc that is often criticized for launching attacks everywhere. Recently, they have been accused of launching concerted efforts to destabilize the G19. Whether they have succeeded in doing so or not is a question reserved for the researchers and thought leaders. Many of them think that pressing economic conditions, political instability and military operations both inside and on war fronts in neighboring countries have shifted the focus from cyber activism.

The discussion and analysis on the scene may give us a faint idea about how the year 2023 would look like.

Russia:
The conflict in Ukraine has strained the position of Vladimir Putin and analysts believe he is losing his grip on power. After almost a year of warfare, Russian economy is suffering badly because of sanctions and trade embargo. Theories abound that some leadership change in Russia might emerge not far away from now.

China
The stringent COVID policy adopted by the government is having its toll and creating upheavals. Internal uneasiness has been felt and China appears to be struggling with internal challenges from the zero-COVID policy, and political discontent within leadership has been observed. The country is making heavy investments for developing advanced new weapon technologies which is unsettling for the US which has remained unchallenged as the super power for a long time.
The global recession and the accompanying economic impacts are not encouraging for Xi Jinping's government. The power struggle has already started and the key player is the policy related to the pandemic.

Iran
Iran is exceeded only by North Korea in terms of the sanctions imposed by world powers. Iran is also branded as an ally of Russia in a war that is considered as illegal. Western media paint a grim picture of the country saying Iran is riddled with a number of problems ranging from misogynist legislation marginalizing women which make up more than half of the country's population, diminishing oil exports and strict sanctions which has badly affected the economy which was once thriving. Skeptics surmise that Iran has all the attributes to become a failed state.

North Korea
Last but not the least is North Korea, which is considered as a proxy of China and Russia. . Arguably a proxy of China's and/or Russia's global machinations, this small nation seems to be playing a game of "look at me" on the world stage, with proactive ballistic and short-range missile launches, as well as a stream of threats to unleash nuclear capabilities on just about anyone in its general vicinity. But as North Korea increasingly becomes eclipsed by other world events, its activities and announcements simply become background noise? These questions, along with a healthy discussion on cyber capabilities, form the main discussion as 2022 comes to an end.

PHISHING ATTACKS

DEEP DOWN EXPLANATION AND DEFENSE STRATEGY

Any hacker who is worth his salt knows very well that professionals like him are enamoured by phishing. Not because the activity itself provides ecstatic pleasure but only because the bait promises extraordinary rewards. If any of the hacker's initial maneuver results in a success, the reward can sky-rocket to several million dollars. That is why most hackers are angling for phishing.

Phishing is a 'socially inducing online attack' that targets unsuspecting people into exposing themselves to various threats by sharing personalized, high value information. Also known as "phishing scam", the phishing attackers aim to acquire, through dubious means, individuals' private and financial information (such as credit cards or bank accounts numbers), corporate records and any other valuable information. Phishing attackers are online con artists.

Business organizations, especially the large ones, have remained the target of phishing attacks keeping in view their volumes and attackers' ability to maneuver through their security protocols. If a team-member falls into the trap of a phishing scam, it can potentially expose the whole team to risks. It is, therefore, need of the hour that business entities take stock of the situation and must assess their preparedness to this threat by adopting penetration testing exercises and onboarding the results through training sessions of workers on digital security.

FUNDAMENTALS

Types of phishing attacks

Basically, 'phishing' usually refers to the act of directing unsolicited communications to a relatively large group of persons with a goal that few of them, at least, get caught in their net. This is done by attracting the target with a very simple initial response despite the fact that the likely benefit for the attacker may not be that significant.

In a typical fashion, phishing messages grab the attention inciting a minimal response (usually a mouse click) by playing with psyche of the target, as in the following examples:

"Last chance to avail 80% discount" (greed)
"Your account has been debited" (confusion)
"Your order will be cancelled if you do not give your confirmation immediately" (concern, sense of urgency)

Email Examples of a Phishing Attack:
Attackers employ multiple methods through a single e-mail message, to gain access to someone's information. But certain tell-tale signs help in knowing if the message is genuine.

With the passage of time, phishing attacks have also undergone transformations and innovations with some attackers now requiring a more complex response, but which also yields a larger volume of victims or a bigger benefit value from victim, or both.

Spear Phishing

Spear phishing is a custom-made phishing attack, directed towards a corporation or certain person(s). These attacks include additional features, collected and assembled for their preparation and incorporate other familiar identity elements like logos, web-domains or other associated undertakings. In some immaculate preparations, the phishing e-mails, with a view to appear as genuine as possible, may also include personal or professional profile of the addressee. This extra preparation often results in desired response from higher number of targets.

Whaling

Whaling is an extension spear phishing, targeting the top management personnel of an entity. Whaling attacks use job profiles of these personnel to design targeted messages. An effective whaling attack can result in access to substantial benefits and data as these executives are likely to hold critical information of the corporations.

Clone Phishing

Clone phishing is one more version of spear phishing where intended victims receive copy of a genuine message already in their record, but with slight malicious modifications in provided attachments or links to achieve the desired response. Since the attacks incorporates a familiar and genuine message, it can be effective in tricking a target.

AND MORE

With each passing day, phishing e-mails keep on targeting unwary persons with evolving and ingenious ideas. Recently, an attack used a Google Doc sent to an identified target, with the aim to get access to user's login details and then spread to other e-mails of user's contacts. There are also other forms of subtle phishing attacks such as pharming, that can create problems for the users just like any other attack.

PHISHING TECHNIQUES

Phishing is not done through e-mails only. The attackers also employ other channels like social media, instant messaging, texting, infected websites and even phone calls. Irrespective of the method adopted, there are some skills required to perform phishing attacks.

Link Spoofing

A commonly used way is to send a harmful weblink in the garb of a genuine one, that would make it more likely for the target to treat it as authentic and accordingly move on to explore. The users who are conscious to 'check before click' can detect such links with ease. Still, there are attacks called homograph attacks, that make use of the similar looking characters interchangeably to confuse the users and neutralize the value of visual identification.

Website Spoofing

Just like the manipulated links, there are also fake websites to trick the users. These sites present themselves as genuine by using tools like Flash or JavaScript that gives attackers control on how the web-address appears in user's view. In this way, the target would believe as though he is visiting an authentic site while being duped on a malicious website. To further enforce this methodology, the attackers use Cross-Site Scripting (XSS) – a tool that identifies and manipulates the weaknesses of a genuine site. The attacker is then able to present the real website with genuine web-link and certificates to silently take away the personalized details provided by users.

Malicious and Covert Redirects

Proficient attackers are able to

assign codes that forces a conscious visit to an authentic website to be redirected to an unexpected, specially designed malicious site that is under the control of the attacker.

On the other hand, covert redirects do not openly allow the targets to realize that they are communicating with malicious sites. A common method in this technique is to insert a new action in an existing website asking the user to log in with his social media account(s) in order to post a comment. This tricks the user to expose his social media login which are then stored at attacker's platform, before continuing to the user's social media page, and therefore, keeping the user in the dark.

HOW TO PREVENT PHISHING ATTACKS

Following are the suggested actions to counter phishing attacks:

Persistent User Awareness and Training
Justin Buchanan, Senior Product Marketing Manager, points out the ways in which employees can identify likely menaces of phishing operations.

Justin Buchanan, Sr Director of Product Management, CISCO, reliable resource in the battle to counter phishing attacks Punctually organize and undertake awareness sessions and regularly remind on how to recognize and stay away from phishing traps, further boosted with periodic but unannounced mock phishing routines to assess the preparedness.

Filter Suspicious Attachments
Remove and quarantine incoming attachments known to be utilized in malicious ways before they reach your users.

Filter on Malicious Links
Isolate e-mails and other communications with suspicious links. Also, ensure clearance of any web-links coming under link shorteners (e.g. bit.ly, goo.gl, etc.) to see that they do not carry malicious content.

Install the latest filter tools based on character recognition in a bid to capture the characters hidden in large images.

Promote Good Credential Behavior
Emphasize and implement adoption of strong passwords that with at least 10 characters having alphabets (both capital and small), numbers, and symbols.

Make it mandatory to frequently change passwords.

Adopt two-step verification (2SV) or two-factor authentication (2FA) solution.

Additionally, it's also good practice to regularly scan user and infrastructure systems for malware and keep them current on software updates/patches.

The breadth of phishing attacks and attack methods out there may sound scary, but with proper training around what a phishing attack is, how it works, and how it can harm users and their organizations, you can help ensure you're as prepared as possible to recognize the threat and mitigate it accordingly.

Insider Threats in 2022

MORE THAN HALF OF ORGANIZATIONS EXPERIENCED THESE

Gurucul is a cybersecurity company geared toward protecting most valuable assets of organizations. Their efforts to shield data and information from insider threats and external cyber attacks have earned considerable following. Recently, they have released a report revealing that insider threats are top concerns for organizations all over the world. Only 3% of organizations surveyed were not concerned with insider threats.

The survey relied on responses from over 325 cybersecurity professionals. The questions explored latest challenges and trends being faced by organizations and how they are adapting themselves to protect critical data and IT infrastructure from insider threats. The ever altering insider threats were found to be of greatest concern among all the surveyed cybersecurity leaders.

Almost 75% of the respondents said that their organization was moderately to extremely vulnerable to insider threats—a significant increase from previous year's percentage. The rise in vulnerability perception can also be attributed to more frequent insider attacks (a 6% increase as compared to last year's figures). The report also highlighted the fact that almost 60% of the surveyed organizations experience at least one attack whereas 25% of organizations faced more than six attacks.

The cloud space is also a challenge for managing security of data and information. Often, organizations do not have access to necessary technical tools to detect and prevent any insider attack. More than 87% of cybersecurity leaders believe that devices, websites, on-site resources and infrastructure should have unified visibility and control. Nearly 50% actually monitor their systems and cloud space for any suspicious activity. And just as many of the respondents were sure that detecting insider threats is not an task in cloud space.
Some other statistics of the report are worth noting:

The top reasons that prevent timely detection and prevention of insider attacks include trusted insiders who already have access to apps, networks and services (54%), liberal use of SaaS apps that can leak data (44%) and an increased use of personal devices having access to corporate resources (42%).
More than 60% of cybersecurity professionals are concerned about insiders like IT users, admins and certain other officials who have access privileges to critical data. Third party contractors and service providers also form 57% of cybersecurity professionals' concerns, followed closely by regular employees (55%) and privileged business users (53%).
With the rise in threats, organizations are compelled to implement insider risk programs. Almost 39% of organizations have already put insider threat programs in place. Another 46% of organizations are moving to add insider threat programs in a short while, which is 5% more than the previous year's share.

The recent worldwide trend in remote working has escalated the risk profile. More than 68% of cybersecurity professionals are worried about insider risks because the post-Covid time may shift to permanent hybrid work model which might increase the risk factors.

PROTECTING WEBSITES

BEST DEFENSE TECHNIQUES

Businesses, large or small, are now anchored to websites or portals. Most service based businesses conduct their operations including public relationing through websites. Online presence has become the order of the day and an indispensable tool to provide competitive edge.

The level of importance gained by websites is routinely watched by threat actors. And they are keen to capitalize on any weakness in the websites. If the security infrastructure has vulnerabilities, hackers will be eager to exploit it to the hilt.

Hackers are nowadays employing newer and more damaging malicious software to make a breach. They are continuously learning to use increasingly sophisticated technology for their purposes. Logically, one would think that more sophisticated methods would have to be employed to protect the websites. But it has been seen that small and simple practices can provide effective security and maintenance for websites.

Here are some simple measures that can mean huge strength for the website.

USING STRONG PASSWORDS.
Passwords are the first lines of defense against illegitimate attempts to get into a system. They are the most common types of authentications in use worldwide because of their simplicity and low cost. Passwords constitute a string of characters which may include alphabets, figures and special characters or a combination of all three.

A strong password provides better security and protection from hackers and their malware. Hackers often use sophisticated software based on 'brute force' which helps in cracking passwords. There are ways to compose a strong password which give a tough time to hackers. A good password is at least eight characters long. And it uses a combination of upper and lower case letters, special symbols and numbers. This password policy should be enforced throughout the organization.

The composer of the password should avoid using predictable words or names or dates. The thumb rule is if a relative or someone close can guess the password in less than twenty attempts then it is not a good password. Same passwords should not be used on different sites because the levels of security

are different. A hacker can crack a password on a site with weak security and use it on other sites where he can access valuable data. Intelligent users not only compose different passwords for different sites, they also change the passwords frequently to minimize any chances of hacking.
It is desirable to read specific guidelines outlined by National Institute of Standards and Technology (NIST). With some basic knowledge about composing a strong password, a user can further improve on it by trying different and more difficult combinations. This would make it almost impossible for an outsider to crack.

UPDATING SOFTWARE. It is critical to update all platforms and scripts. Outmoded WordPress files are one of the most vulnerable and that is the key reason most websites operating on WordPress platforms get breached. Hackers are fond of exploiting security flaws in popular software. These software should be routinely updated to patch security holes. And this includes WordPress themes and plugins present on a website. It is also important to delete unused themes and plugins because they too become vehicles for carrying malicious software on websites.

ENCRYPTING LOGIN PAGES. SSl certification adds a green padlock to the browser's address bar and encrypt the data being transmitted. This provides security to sensitive information like credit card numbers, social security numbers and login details while these are being shared or transmitted. SSL also makes sure that the information that is encrypted means nothing to third party. Even when it is intercepted, it remains safe. Hackers find it almost impossible to access login credentials or other private data. SSL certificates are also helpful in avoiding unsafe websites which might have a negative impact on search engine optimization.

KEEPING WEBSITE CLEAN.
Databases, applications and plugins are all helpful in performing tasks. At the same time they are a liability too because they are also entry points of malware. Good website maintenance consists of de-cluttering the site of spurious elements. Any files, databases, software, or apps that are no longer in use should be consigned to the bin. This is helpful in keeping things organized.

BACKING UP THE DATA. In this age of frequent hacking incidents, having a backup of data is of paramount importance. In case an organization's (especially the one running an online business or providing a service) website is hacked, the data backup would enable the organization to get the site up and running.
Although the web hosting service running the site should provide backups on their servers, organizations should still maintain their own backups with regular updates. Some content management packages also have plugins or extensions that automatically backup the site. Having that facility should not stop an organization from maintaining its own backups.
An easy way to start a backup is to activate the feature in ManageWP dashboard which ensures that data is backed up at least once a month. The backup feature has an added advantage: it allows the organization to restore the site with a single click.

SCANNING WEBSITE FOR VULNERABILITIES. It is essential to regularly carry out internet security scans to test for internet site and server vulnerabilities. Scanning can be performed easily of malware, blacklists, and errors at any time by utilizing Security Check features in Manage WP dashboard. Web security scans should be scheduled at regular intervals or after every change or addition in web components. A number of tools is available on the internet which can measure how secure a particular site is. Most of them are free and are of great help for briefly reviewing the status of the site but these can be upgraded to facilitate daily and weekly checkups in an easy way.

HIRING A SECURITY EXPERT.
As stated above some of the tools that are freely available can perform brief reviews but they are not capable of in-depth analysis. Detecting all possible flaws and threats on the site is beyond those low-level software. But having a professional to perform security checks at regular intervals is a better approach.

Another alternative is to hire the services of a firm that provides security services. While the routine stuff can be handled by the staff at the workplace but some security measures require the attention and expertise of professionals. By hiring such a service, an organization can free itself of the need to scan the website for vulnerabilities, perform security audits, monitor suspicious activity and be on guard whenever repairs are required. This is the shortest and most effective path to remaining ever vigilant in security matters.

BEEFING UP THE DEFENSES.
Although these simple steps, if practiced religiously can deliver the desired protection but sophistication and hackers' techniques are boundless and there is always a chance that some new method would be contrived to make an onslaught. Cybersecurity

experts, therefore, suggest some more techniques to beef up the security.

MULTI-LAYERED SECURITY. With this strategy in place, several layers of defenses work in tandem to protect the entire system. To help counter any flaws and gaps in defense, every layer aims to protect access points of a specific area. All the layers work together to tighten the defenses. Each layer ensures an additional level of protection. This implies that more layers will provide better defense, making the hackers' task a bit arduous. With enough layers, organizations can very effectively block the entry of hackers in their system. Often, this layered approach is helpful as opposed to one which uses a single security solution.

DEFENSE-IN-DEPTH. NSA, the US National Security Agency, conceived the concept of in-depth defense by drawing inspiration from a military strategy that shares the same name. This method of defense is sometimes referred to as a 'Castle Approach' after the layered defenses of medieval castles which featured moats, drawbridges, steep walls and towers.

The defense in depth approach spans people, technology and operations. It is a combination of guidelines and best practices aimed at protecting infrastructure, processes and systems.

ZERO TRUST SECURITY. This approach is based on the premise that no one from inside or outside is trusted. With zero trust approach in place, everyone desiring to gain access to any area of the system or to network resources must provide identity verification. This approach does not make any distinction between an outsider and an insider. Zero trust approach makes use of various technologies like analytics, orchestration, permissions, encryption, identity access management, multi-factor authentication (MFA), and risk analysis. Governance policies also play a key role in making the security system a successful model.

WAF SECURITY. WAF is short for web application firewall. It is a means of protecting web applications by filtering and monitoring http traffic. WAF shields web applications from attacks such as cross-site forgery, cross-site scripting and SQL injection. Although WAF is not designed to provide defense against all types of attacks, it does however mitigate risks by neutralizing certain types of threats and acts as a component of a holistic defense mechanism against a range of attack vectors.

THREE-TIER ARCHITECTURE. This type of security provides a great degree of flexibility to organizations that are planning to adopt new technology when it is available. The key components of this architecture remain intact while the system, as a whole, keeps evolving organically. The 3-tier architecture provides great freedom to development teams who can update or replace only specific parts of the application without affecting the product as a whole.

The three tiers include:

Presentation Tier: It is the topmost tier displaying information in the form of graphical user interface (GUI). This front end layer, which end-users interact with directly, is built on web development frameworks such as CSS or JavaScript

Application Tier: This tier is known by several names: middle tier, logic tier or business logic tier. It aims to control the application's core functionality by performing detailed processing. To make this tier functional, coding is done in programming languages such as Python, Java, C++, .NET and others.

Data Tier: In this tier, the stored data remains independent of application servers or business logic. Programs like MongoDB, Oracle, MySQL and Microsoft SQL Server are used to manage and access the data.

INCIDENT RESPONSE AND THREAT INTELLIGENCE. In today's complex environment, organizations cannot afford to relax or be casual. They have to be vigilant against security threats. To counter all sorts of threats, it is important to have a robust incident response plan. And that plan relies on a strategy that covers situations 'before', 'during' and 'after' a breach.

To minimize revenue loss of a security incident, organizations require a comprehensive plan that integrates security threat intelligence, incident response and remediation.

Websites are most important online business assets. They should be protected and guarded with the same fervor and alacrity as one would guard real estate. A strongly secured and properly maintained website will provide a safe environment for the customers and enhance the rating of the website. This means profits and greater acceptance among the masses. Once these guidelines and best practices discussed above are adopted, a near impregnable security—as effective as99.99%—is assured.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

Online Safety Basics

With a little prep, you can shield your information online and secure your digital systems and devices.

Literally, a few minutes of preparation can keep you safe. The benefits of a few moments of research, preparation, and action far outweigh the potential costs of losing your unprotected data in a breach or having your identity stolen. And even if some of your data is compromised, you can ensure that the damage will be minimal by following some simple guide lines:

KEEP A CLEAN MACHINE
CREATE LONG, UNIQUE PASSWORDS
USE A PASSWORD MANAGER
ENABLE MULTI-FACTOR AUTHENTICATION
THINK BEFORE YOU CLICK
REPORT PHISHING
USE SECURE WI-FI
BACK IT UP
CHECK YOUR SETTINGS
SHARE WITH CARE

Contact us at +92-21-34325505,
Email : info@diginfo.net | www.diginfo.net

SCAN ME

Guess The Word

A WORD ABOUT THE MOST USED PASSWORD

A large majority of people chooses words, phrases and combinations of characters for their passwords. While making the choice, most people, however, ignore the advices often repeated by cybersecurity professionals. This leads to liberal use of common, day-to-day words, phrases and alphanumeric characters that have become so popular that hackers won't even have to scratch their heads to break the secret.

Every year, independent researchers conduct surveys to find out the most used passwords. And every time strange results emerge. Heading the list of common passwords in the year 2022 was 'password.' Globally, the 'password' password was used nearly 5 million times—4,929,113 to be exact. This was followed by 123456, which was used 1,523,537 times.

The list of top five most common passwords on global scale are:

- password: 4,929,113 times
- 123456: 1,523,537 times
- 123456789: 413,056 times
- guest: 376,417 times
- qwerty: 309,679 times

The list of common passwords for the US is different but reflects some similarities:

- guest: 127,861 times
- 123456: 109,322 times
- password: 74,533 times
- 12345: 31,675 times
- a1b2c3: 15,702 times

Researchers have noticed that a huge number of people think alike while choosing a password. There is a pattern in the thought process and it is easily recognizable and predictable. This trend is not a good sign and it exposes individuals and organizations to attacks. A good many ransomware attacks begin with a breach in email accounts.

To ward off such threats, experts give three key suggestions, besides several others, which can provide data and information safety to a great extent.

PASSWORDS SHOULD BE LONG. A complex password usually contains 12 or more characters. And these characters may consists of letters (both upper and lower case), numbers and symbols. The greater the complexity, the more difficult it is for hackers to crack the secret.

PASSWORDS SHOULD NOT BE REUSED. Using the same password on different sites and accounts is not a good idea. It makes the job of a hacker all the more easier. Once he succeeds in breaking into an account, he will try his luck with the same decoded password on the victim's other accounts.

PASSWORDS SHOULD BE AUDITED. Keeping track of used and unused accounts is a good practice that may save people from headaches. Unused accounts should be closed if the user does not intend to use them for an extended period. Unused and unattended accounts often give an unhindered path to hackers. Users cannot detect any suspicious activity if they do not often access their account.

PASSWORD STRENGTH SHOULD BE CHECKED AND UPDATED. Assessing password health is key to effective data management. The practice conducted regularly goes a long way in building a safety barrier around data and information. Old, weak and overused passwords should be promptly discarded and replaced by newer and more complex ones.

LEFT OPEN SCADA NETWORKS

SEAMLESS EAVESDROPPING BY CRIMINALS

Life on our planet is replete with dual standards. At some places, the whole world seems to attach extra importance to a particular aspect. At others, we turn a blind eye and give scant attention. A glaring example is the case of unattended baggage on airports. The staff keeps a vigilant eye on baggage that is left unattended. Loudspeakers blare and security officers reach the spot in a blazing fast action to inspect if there is any threat.

On the other side, there are instances when a lot more is at stake and no security or vigilance is exercised. Large industrial setups and huge power plants work fine without ongoing control and surveillance—unlike the way we see at airports and public spaces. It has come to notice of analysts and observers that operators at power plants and industrial units leave some of the main components alone and unattended. That carelessness can mean grave consequences.

Essentially, we are talking about Supervisory Control and Data Acquisition (SCADA) networks. Before delving into the issues associated with such networks, a good approach is to start with the basics.

BEGINNING WITH THE ABCs.
SCADA systems are combinations of software and hardware elements that allow large industrial organizations to perform automated tasks:

- Control industrial processes locally or remotely.
- Monitor and process real time data.
- Interact with a variety of industrial devices through HMI software.
- Maintain a record of process events in a log file.

The earliest examples of SCADA systems can be traced back to the 1950s when computers were first developed for industrial control purposes. The efficiency of industrial processes quickly showed an upward climb as the use of SCADA networks became common. In the next decade, telemetry was devised for monitoring purposes. This facilitated automated communications which ensured transmission of measurements and allied data from remote locations to monitoring equipment. The term SCADA was coined in the 1970s which coincided with the development of microprocessors — critical components of monitoring and control systems.

The popularity and extensive application of this system in large industrial setups dates back to this period.

In its simplest form, a SCADA architecture consists of Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) which are microcomputers designed to communicate with other components of the network such as HMIs, sensors and end-devices. PLCs and RTUs gather information from these components and communicate to the network where it is processed and displayed. Operators and technicians can then analyze the readings to make key decisions and regulate the entire industrial processes.

THE EVOLVING PHASE: During the early period, SCADA systems worked in conjunction with mainframe computers. Networks had not yet made their mark back then and each SCADA sytem was a stand-alone entity. Such system came to be known as monolithic SCADA systems.

Things began to change in the following decades when smaller and portable computers were introduced and accepted as useful tools to perform various tasks related to industrial processes. Besides these, LAN networking and PC based HMI software also played an important role in popularizing the SCADA systems. However, not all LAN protocols were proprietary meaning vendors exercised control over the system and had the liberty to optimize data transfer. These systems, known as Distributed SCADA systems, were evidently incapable of communicating with other vendors.

Further down the road, in the late 1990s and early SCADA systems went through an incremental change by embracing an open system architecture and communication protocols which were not specific to a particular vendor. The new SCADA systems came to be known as Networked SCADA systems. The networked systems accommodated communications from other vendors and by making liberal use of Ethernet, the new SCADA systems ensured that more devices are able to connect to the system.

MODERN SYSTEMS: In the early part of this century, SCADA developers could not keep pace with the sweeping changes in technology. At that time, Structured Query Language (SQL) became the choice for managing IT databases. SCADA developers put up a resistance and did not adopt the language for standardizing their systems. This resulted in a sluggish performance by SCADA systems because they used outmoded proprietary technology which was too expensive and too messy. This paved the way for modernization efforts to bring the technology at par with new demands. Today, SCADA systems employ best features of IT technology together with ultimate controls which have solved many of the problems that are faced by large industrial processes.

SCADA systems these days offer real time data for access. Any authorized person can gain access to the data from anywhere in the world. This facility provides a great advantage to governments, businesses and individuals to make informed decisions by gaining access to real-time data and improving the processes. Without SCADA at work, this would not be possible.

SCADA systems also have another great merit. They possess a feature called Rapid Application Development (RAD) which enables any operator to design and make changes to applications relatively easily even if software knowledge and coding is lacking.

SQL and web based apps have also enhanced capabilities of SCADA networks. With the introduction of SQL and modern IT standards, the

SCADA systems have become more efficient, productive and reliable. One key advantage of drawing the benefit of Structured Query Language is that integration of MES and ERP becomes a breeze. This facilitates easy flow of data across entire segments of an enterprise. Old data of SCADA system can also be logged in to SQL database which facilitates data analysis by way of data trending.

RISK POTENTIAL: SCADA networks are responsible for performing a number of tasks. Their roles and functions include monitoring, analysis and exercising control on infrastructures, IT systems, applications and computer hardware. The system also has an eye on automated processes, devices and industrial equipment installed locally or at remote locations.

The security of SCADA networks is a complicated affair because the network in involved in a variety of different activities. From IT systems and software applications to physical components and remote terminal units (RTUs), everything falls under the watchful eye of the SCADA network. This represents a large attack surface area and, evidently, the network is exposed to a volley of attacks because of multiple threats.

The risk potential of SCADA systems is constantly on the rise. The phenomenal growth in information technology is contributing towards this escalation. In earlier times, SCADA systems were autonomous and the number of persons who had the right to access the data was restricted. That is why the threats were few but now the attack surface is huge. And the spectrum of attackers is equally wide ranging from malware to state-sponsored foreign actors. The methods also vary in shapes and sizes like malware or DoS attacks which work with the objective of getting illegitimate access to data, destroying or altering the infrastructure, blocking services or introducing malfunctions.

COUNTING VULNERABILITIES: There are two distinct threats that can affect modern SCADA systems. The first one is the threat of unauthorized access to the control software, whether it is human access or changes made deliberately or unintentionally by virus infections and other software threats existing on the control host machine. The second is the threat of packet access to the network segments hosting SCADA devices. In particular, security researchers are concerned about security and authentication in the design, deployment, and operation of some existing SCADA networks. Moreover, they need to also take into consideration whether the SCADA networks are secured just because they are physically disconnected from the internet. In addition, security researchers are also concerned about the existing security and authentication protocols in the design, deployment, and operation of SCADA networks, with the belief that SCADA systems have the benefit of security, obscurity through while using specialized protocols and proprietary interfaces. Besides these two, cybersecurity experts who study SCADA networks have identified common vulnerabilities which entice criminals to constantly stalk the systems for a possible attack. The purpose of identifying these threats is to ensure that every industrial enterprise takes extra care and exercises extra vigilance for security purposes. Here is the list that would be helpful for tech experts who run SCADA networks for monitoring industrial processes. Here 's a list of Donts:

- Lack of policies, procedures, and training related to SCADA systems.
- Weak network architecture with no depth in defense.
- Unprecedented increase of traffic between process and office networks.
- Liberal use of unprotected remote access and insecure transmission protocols.
- Lack of protection for physical access to systems, networks, and transmission facilities.
- Lack of protection against malware.
- Lack of safety awareness among operators and suppliers.
- Easy availability of information about architecture, mode of operation, networking and communication technology.

FINDING SOLUTIONS: To counter the variety of threats, following security measures of SCADA systems can help protect the network in conjunction with the corporate network:

- Strict restrictions and authority control are needed for external connections.
- Reinforced security for systems in demilitarized zones and internal network.
- Extra security using virtual private networks besides integrity tools of servers.
- Minimal access paths to the internal network and enhanced concentration of monitoring.
- Encryption of emails and locking of files and directories.
- Regular and thorough inspection of security and vulnerability.
- Development of control and monitoring methods to cope with unexpected situations in the SCADA equipment.

SCADA systems have acquired a crucial status for industrial organizations. These systems maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime. Their ability to notify the operator of an issue can be a great help to resolve it and prevent further loss.

If proper security measures are put in place to check seamless eavesdropping by cyber criminals, SCADA systems have all the attributes to turn themselves into an asset for an industrial enterprise, despite all the odds.

Ferrari Confirms Cyber Incident

ATTACKERS ACCESS COMPANY'S SYSTEMS

Italian automaker has admitted of a ransomware attack. A gang of hackers that identifies itself as RansomEXX has stolen 7GB of data including internal documents, data sheets and repair manuals.

Although the company has confirmed that a cyber incident had taken place, there is no conclusive evidence of data breach. What's more there is no disruption in the business of the automaker.

The threat actors have placed a ransom demand soon after stealing the data but Ferrari has flatly refused to accede to the ransom demand. Instead, the company has hired the services of cyber security experts to investigate the crime.

In a statement released just days after receiving the ransom demand, Ferrari spokesman asserted the company's stance in these words, "As a policy, Ferrari will not be held to ransom as paying such demands funds criminal activity and enables threat actors to perpetuate their attacks. Upon receipt of the ransom demand, we immediately started an investigation in collaboration with a leading global third-party cybersecurity firm. In addition, we informed the authorities and are confident they will investigate to the full extent of the law."

In a communique to the clients, the CEO of Ferrari, Benedetto Vigna sent out the following message to restore confidence:

Dear Ferrarista
We regret to inform you of a cyber incident at Ferrari, where a threat actor was able to access a limited number of systems in our IT environment. As part of this incident, certain data relating to our clients was exposed including names, addresses, email addresses and telephone numbers. Your data may have been included as part of this incident. However, based on our investigation, no payment details and/or bank account numbers and/or other sensitive payment information, nor details of Ferrari cars owned or ordered have been stolen.

Cybersecurity experts from all over the world have welcomed the automaker's decision to refuse ransom payment. There is unanimity in the cybersecurity circles that surrendering to the demands of hackers only emboldens them and helps fund their malicious activities. Moreover, the ransomware threat actors often turn back on the agreement and do not surrender the stolen data. There are just no guarantees. The best approach is to report the crime to the law enforcement authorities and wait for development.

This was not the first time Ferrari faced a breach. As recently as October 2022, the company was targeted by a group known as RansomEXX. Some investigators have surmised that the same group might have had some role in latest attack. So far, the hackers' identity has remained elusive.

In spite of the firm stand by the automaker, there is apprehension among customers that the stolen data can find its way to the dark web where it can be misused to commit further crimes like identity theft and fraud. This seems to be a distinct possibility as the owners of Ferraris are no ordinary citizens. Their net worth can be a huge motivation for the threat actors.

DG ACADEMY

INTRODUCING

DG NSOS

SECURE OPERATING SYSTEM

TRAINING PROGRAM

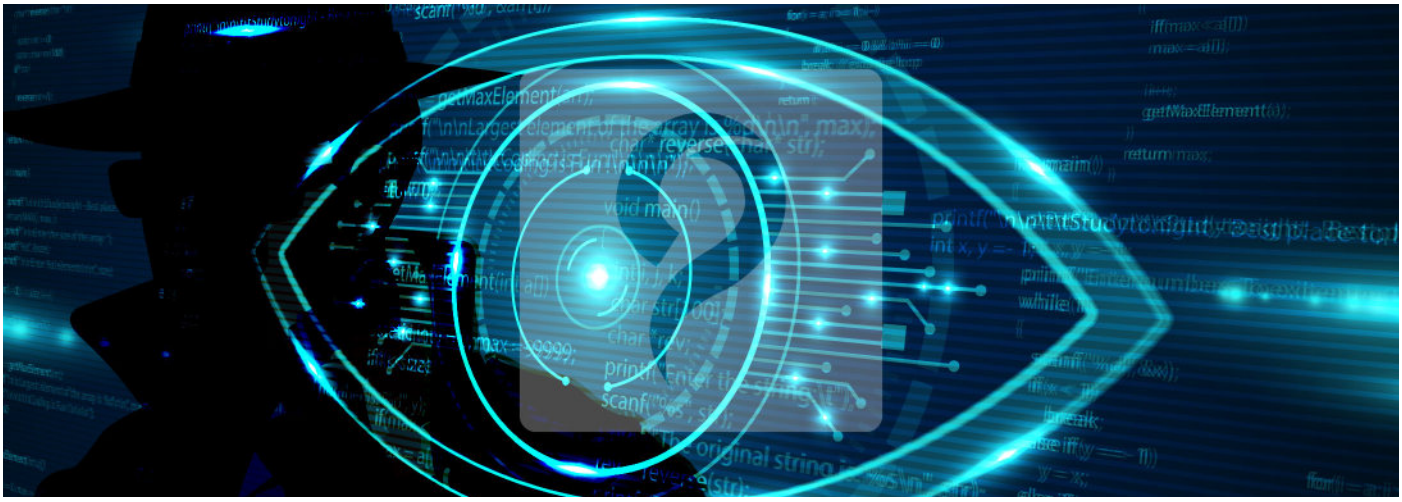
Stand out from the crowd by mastering professional Linux in no time

https://dgacademy.diginfo.net/dgnsos/ ENROLL NOW

For further detail contact: +92 300 254 2564

Cyber Crime and Cyber Espionage

OVER $100B LOSSES ESTIMATED



The Center for Strategic and International Studies (CSIS) and McAfee have jointly conducted a study which is titled as "Estimating the Cost of Cybercrime and Cyber Espionage.' After careful analysis and painstaking surveys, the researchers have put a staggering cost of cyber crime to the US national economy. The figure is $100billion—easily surpassing the annual budget of several countries.

The researchers have also revealed that 508,000 jobs are lost in US because of malicious cyber activity. According to the study, which is entitled 'Estimating the Cost of Cybercrime and Cyber Espionage', as many as 508,000 jobs in the U.S. are lost as a result of malicious cyber activity.

According to the study, "While this translates into a third of a percent decrease in employment, this is not the "net" loss as many workers will find other jobs.The real concern might be if the lost jobs are in manufacturing or other high paying sectors. If workers displaced by cyber espionage do not find jobs that pay as well or better, the victim country would be worse off."

James Lewis, Director and Senior Fellow of Technology and Public Policy Program at CSIS, and a co-author of the report, says, "Using figures from the Commerce Department on the ratio of exports to U.S. jobs, we arrived at a high-end estimate of 508,000 U.S. jobs potentially lost from cyber espionage. As with other estimates in the report, however, the raw numbers might tell just part of the story."

While calculating the costs of malicious activity, the researchers have taken into account several factors resisting the urge to restrict the study to financial losses alone. Therefore, the estimate includes losses to intellectual property, damage to brands, consumer losses from fraud, and various other costs. The researchers divided the malicious cyber activity into following areas:

- Loss incurred on intellectual property.
- Cybercrime.
- loss of sensitive business information, including possible stock market manipulation.
- Opportunity costs, including service disruption and reduced trust for online activities.
- Additional costs of securing networks and reputational damage to the victimized company.

Mike Fey, Executive Vice President and Chief Technology Officer at McAfee has issued a statement which asserts, "We believe the CSIS report is the first to use actual economic modeling to build out the figures for the losses attributable to malicious cyber activity."Other estimates have been bandied about for years, but no one has put any rigor behind the effort. As policymakers, business leaders and others struggle to get their arms around why cyber security matters, they need solid information on which to base their actions."

IS ENCRYPTION DEAD

CHALLENGES AND SOLUTIONS

Three years back, the then Attorney General of United States, William P Barr, reignited the debate on security versus privacy. He asserted that encryption effectively turned computer systems and devices into ‘law-free zones.’ He considered that these zones kept law enforcement officials out and hampered criminal investigations. In his keynote address at an International Conference on Cybersecurity (ICCS), he said, “As we use encryption to improve cybersecurity, we must ensure that we retain society’s ability to gain lawful access to data and communications when needed to respond to criminal activity.

WAR OF WORDS.

Barr’s arguments aren’t new. They have been raging for almost thirty years. It is a tussle between the law enforcement organization aiming for investigative powers and cybersecurity community aiming to resist any external control on privacy matters.

The cybersecurity community reacted sharply to Barr’s statements saying that he “has a completely wrong-headed take” on the issue. Max Kaufman, senior staff lawyer in the Center for Democracy at the American Civil Liberties Union, said, “Encryption reliably protects consumers’ sensitive data. There is no way to give FBI access to encrypted communications without giving the same access to every government on the planet. Technology providers should continue to make their products as safe as possible and resist pressure from all governments to undermine the security of the tools they offer.”

Riana Pfefferkorn, associate director of surveillance and cybersecurity at the Stanford Center for Internet and Society said, “Mr Barr is assuming that the negative impacts of encryption on law enforcement investigations far outweigh encryption’s benefits for protecting individuals, business and the nation. That assumption has never been borne out by evidence in the form of actual, accurate numbers about encryption’s effect on law enforcement’s ability to solve crimes.”

To know exactly why there is a standoff between government and technology experts on this particular subject, we must first try to understand what encryption really is.

BASIC CONCEPTS:

Encryption is the key element of data security. It is a simple mechanism to protect computer systems from theft.

Encryption in cyber security is the conversion of data from a readable format into an encoded format. Encrypted data can only be read or processed after it's been decrypted. Encryption is the basic building block of data security. It is the simplest and most important way to ensure the safety of a computer system's information. With encryption, data can't be stolen and read by someone who wants to use it for malicious purposes.

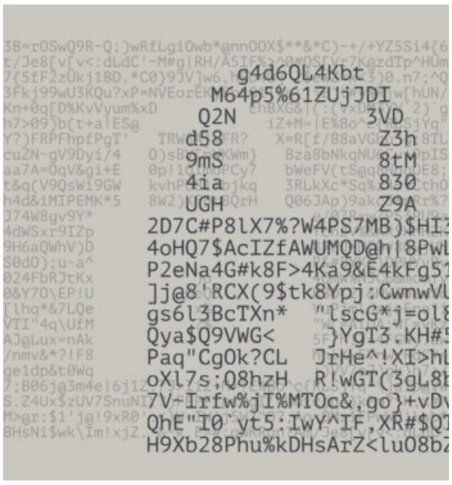
Data security encryption is widely used by individual users and large corporations to protect user information sent between a browser and a server. That information could include everything from payment data to personal information. Data encryption software, also known as an encryption algorithm or cipher, is used to develop an encryption scheme that theoretically can only be broken with large amounts of computing power. It is also an effective measure to stop someone who wants to use the data for malicious purposes.

Encryption constitutes conversion of data from a readable format into "ciphertext" which can't be deciphered without a decryption key or a password. To protect critical data from unauthorized access, modification or theft, sophisticated encryption solutions together with effective key management is offered. Data encryption is useful both for stored data and also for data that is being transmitted from one device to another.

Two types of encryption methods are common in cybersecurity circles nowadays:

Symmetric Encryption consists of key algorithms that use a single key to encrypt and decrypt data. Although this form of encryption ensures fast and efficient handling of data and effective key management, special care has to be exercised. Only authorized and trusted persons should be given the access to encryption key because that key can be employed to encrypt data and also modify and re-encrypt the data without anyone noticing what is going on.

In contrast, Asymmetric Encryption key algorithms use two mathematically related keys. The purpose of one key, often referred to as the 'Public Key' is to encrypt the data. The other key, known as the 'Private Key' is different from the first and it is used to decrypt data. The distinct benefit of this arrangement is that the Public Key can be used liberally for encrypting the data whereas the 'Private Key' can be used only by a few authorized and responsible persons of the organization.



SNOWDEN UNDER RADAR: The 'Privacy Vs Legal Authority' debate again shot to worldwide attention when in 2013, Snowden revealed that National Security Agency (NSA) of the US and Government Communications Headquarters (GCHQ), UK's intelligence, security and cyber agency secretly ran classified intelligence gathering surveillance programs without disclosing the fact to the people. The expose turned into a controversial subject as his supporters claimed that he is a hero while the adversaries branded him as a traitor who should be incarcerated. Snowden himself thought that his revelations had a positive impact on the raging debate. In an interview with the 'Guardian' of UK, Snowden said, "We live in a better, freer and safe world because of the revelation of mass surveillance." Snowden had to flee his country and till today remains in self-imposed exile as the US government framed espionage charges against him. The government functionaries routinely claimed that the computer expert and contractor working for NSA, had violated the law.

In 2013, Snowden revealed the existence of previously classified mass intelligence-gathering surveillance programs run by the U.S. National Security Agency (NSA) and the U.K.'s intelligence organization, Government Communications Headquarters (GCHQ). For this, Snowden was charged with espionage by the U.S. government and, subsequently, be fled the country.

The New York Times stated that, "He may have committed a crime… but he has done his country a great service." In the same newspaper, Ed Morrissey thought of him as a person who broke the law. He asserted that Snowden should be prosecuted for his actions.

ANOTHER FAMOUS CASE : While Snowden's case was still in the news, another case emerged locking Apple and the US government's FBI in a heated controversy. In December of 2015, a terrorist attack in San Bernardino, California left 14 people dead. The FBI seized an iPhone from one of the attackers and attempted to gain access to the data stored on the device. The encryption software prevented the technologists of FBI from gaining access. Initially, engineers from the technology company and the FBI fully cooperated to recover data that was available. But when the FBI produced a court order persuading Apple to help the FBI in unlocking the phone, which meant creating a backdoor to retrieve encrypted data, the CEO of Apple, Tim Cook, backed out and publicly challenged the court in an open letter—dated February 16, 2016—which can be read here: https://www.apple.com/customer-letter/

The website of Apple has presented two key reasons for refusing to cede to the court order:

"This has two important and dangerous implications: … The passcode lock and requirement for manual entry of the passcode are at the heart of the safeguards we have built in to iOS. It would be wrong to intentionally weaken our products with a government-ordered backdoor. If we lose control of our data, we put both our privacy and our safety at risk.

Second, the order would set a legal precedent that would expand the powers of the government and we simply don't know where that would lead us. Should the government be allowed to order us to create other capabilities for surveillance purposes, such as recording conversations or location tracking? This would set a very dangerous precedent."

Both the sides stood the ground and offered their arguments in support of their stance. Those in favour of the Justice Department believed that the US legal system put constraints on government's free access to data. They believed that the question of abuse would hardly surface in the presence of such strictures. Besides, such extreme steps would be inevitable to check crimes of heinous and violent nature like terrorism, drug trafficking and child abuse. The critics rejected Apple's stance arguing that the company was unpatriotic by refusing to comply with the court orders and only harbored an interest in protecting its brands.

On the other side, Apple and its supporters like technology giants, Google and Facebook, reasserted that the court order compelled the company to rewrite the iOS which is akin to violating the First Amendment Right to Free Speech. This meant stating something which is not intended. Also, creating such a backdoor creates a chance that unscrupulous elements like the hackers and cyber criminals may take advantage of it and threaten millions of iPhone users' data. Furthermore, the order would virtually make the technology companies subservient to government orders.

On an enquiry if it is technically possible to do what the government has ordered, the Apple website offers this explanation:

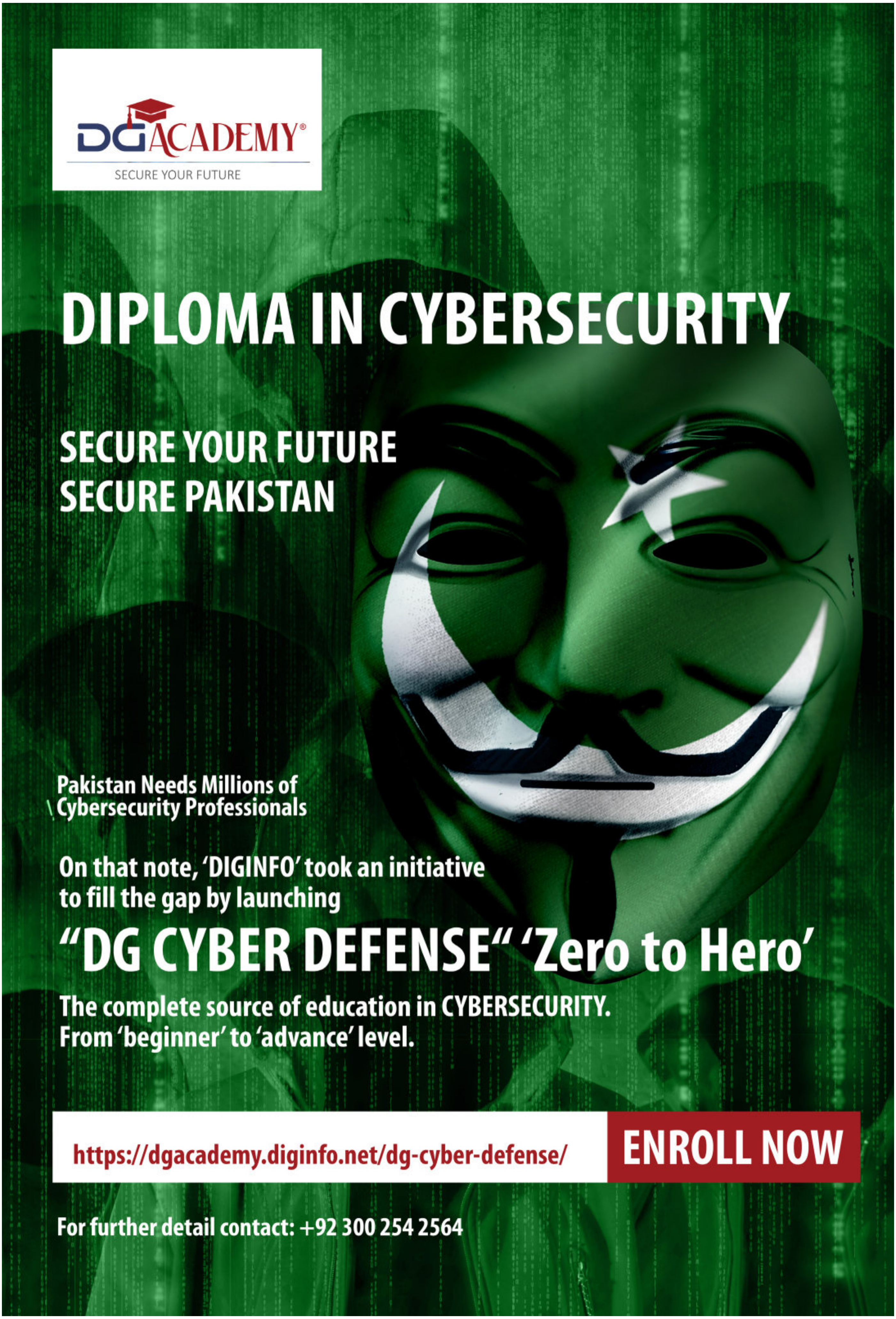
"Yes, it is certainly possible to create an entirely new operating system to undermine our security features as the government wants. But it's something we believe is too dangerous to do. The only way to guarantee that such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it."

The FBI eventually dropped the case because it was able to access the data by breaking in the encrypted code without the company's help. Journalists investigating the developments in the case have reported that the government has paid as much as US$ 1.3m to create a backdoor and unlock the seized device.

In the midst of these events another happening further added fuel to the heat. The Australian parliament passed a bill requiring technology companies to provide law enforcement authorities and security agents with access to encrypted communications. This stirred several technology companies to sign a letter criticizing the new Australian legislation. Among the signatories were names such as Amazon, Facebook and Google.

In recent years, malware has shaken cryptography and data security to a great extent. Particularly grave are the Advanced Persistent Threats (APTs). Some analysts were so enamored by the situation that they hastily started claiming that cryptography is dead. Or at least close to its end. Their argument was based on the belief that APTs wielded the power to watch everything in a system challenging the core premise that hackers can't gain access to encrypted data. But technology gurus contend that there is no need to despair so quickly. Only a slight change in looking at things and adapting to newer ways can make encryption effective and a lot safer. In a conference held some time back, Scheneir, the cyber security expert and author of several books, had this to say:

"We know that technology democratizes. Today's secret NSA program, becomes tomorrow's PhD thesis, becomes the next day's hacker tool."



Cyber Security Conferences

MUST-ATTEND LIST FOR 2023

Security and risk management has become a hot topic of discussion around the globe. Leaders of this area are constantly alert and feel the pulse of what is going around. Conferences are a great source of widening the horizon and keeping pace with the current developments. Cyber security experts and industry professionals waste no time to attend an event if it offers a chance to enhance skills and understanding of the subject.

Here is a list of important events that should be marked on the calendar.

ASIS, Europe
Rotterdam, Netherlands and Online March 21-23 in person, March 2 and April 27 online
ASIS Europe is the meeting place for cybersecurity leaders from all across Europe and beyond. Aspiring professionals together with established leaders congregate to discuss and dilate upon issues of the ever changing threat landscape.

ISC, West
Las Vegas, Nevada, USA
March 28-31
Of all the security conferences held in North America, this one is easily the most well-attended. Security professionals, tech experts and industry thought leaders find time for the event to share ideas and debate on problems pervading the industry. The conference is popular because of several attractions. It includes networking sessions for new professionals, educative and informative programmes and keynote addresses from prominent security leaders.

RLPSA Annual Conference
Denver, Colorado, USA
April 2-5
The abbreviation stands for Restaurant Loss Prevention and Security Association. The conference organized every year offers opportunities of networking to restaurant security professionals. Those attending the conference get a chance to share their experiences and insights related to the industry. This sharing of information is a great way to strengthen and modify the state of security in the hotel and restaurant business.

The Security Event
Birmingham, England
April 25-27
Enterprise and public sector security professionals congregate at Birmingham's National Event Centre to investigate about the new security technologies. The Security Event is designed to address problems of a number of industry niches. What's more, other events like the fire safety conference are also hosted along with the security event.

IAHSS Annual Conference & Exhibition 2023
Nashville, Tennessee and online
May1-3
Professionals and leaders related to healthcare security often take upon themselves to attend the International Association for Healthcare Security & Safety (IAHSS) Annual Conference and Exhibition. This event allows the professionals to network with fellow professionals and learn about

the threats—both emerging and enduring. Furthermore, the event also includes keynote addresses on topical issues—like workplace violence—by industry leaders.

IFCPP 24TH Annual Conference
St Petersburg, Florida and Online
May 6-10
The International Foundation for Cultural Property Protection (IFCPP)'s 24th Annual Conference, held at the Salvador Dali Museum in St. Petersburg, creates a space for interorganizational learning as security leaders from museums, universities and other cultural institutions gather to discuss security strategies specific to the field.

SIA GovtSummit
Washington DC, USA
May 16-17
Government security leaders convene at the SIA GovSummit each year. The 2023 event features keynotes from industry leaders at U.S. Customs & Border Protection, the Department of Homeland Security, the D.C. Homeland Security & Emergency Management Agency, and more.

IFSEC International Security Event
London, England
May 16-18
Co-located with events on fire safety, intelligent buildings, health & safety, and facilities, IFSEC Global's International Security Event serves as a reunion of security leaders from across the globe responsible for international security at their organizations.

NCS4 Annual Conference
San Antonio, Texas
June 27-29
More than 500 sports safety professionals convene each year at the NCS4 Annual Conference, taking place this year in San Antonio, Texas. Event & facility safety leaders will present panels and lead discussions on themes affecting the industry in the past year, from how to mitigate emerging threats to strategies for patron protection.

GSX
Dallas, Texas
September 11-13
The Global Security Exchange (GSX) conference from ASIS International unites security and technology leaders to discuss the newest trends and security challenges seen across the world. This year's conference will feature a large exhibit hall and information sessions, as well as networking events.

International Security Expo
London, England
September 26-27
The International Security Expo is a global conference for security professionals at all stages of their careers, from entry-level professionals to seasoned executives. Government and private-sector security leaders engage with each other and explore new technologies and security strategies at the event.

CONSULT
Louisville, Kentucky
October 13-16
CONSULT is an annual event hosted by SecuritySpecifiers and geared towards security consultants. Conference attendees can explore cutting-edge technologies and their implementations across sectors, featuring a number of informational panels and discussions from industry leaders in technology, consulting, cybersecurity and more.

Securing New Ground
New York City, New York
October 17-18
Entrepreneurs, security executives and those on the cutting edge of the industry meet at the Securing New Ground (SNG) conference from SIA to identify new trends in security threats and strategies.

SECURITY 500 Conference
Washington, D.C.
November 13
The 15th annual SECURITY 500 Conference from Security magazine will take place this November in Washington, D.C. The event features panel discussions and keynotes from a number of influential physical security and cybersecurity executives and unites government and private sector security leaders.

OSAC Annual Briefing
Washington, D.C.
November 14-16
The Overseas Security Advisory Council unites high-level government security and enterprise security leaders for an event geared towards information sharing, learning and exchange. This year's event will see security leaders discussing lessons learned in 2023 and new strategies for dealing with global threats.

Global Count of Ransomware Attacks

STUDY REVEALS SURPRISING STATISTICS FOR 2022

If one cyber crime could be singled out as the most devastating then ransomware would be miles ahead of other crimes. Ransomware not only causes huge monetary losses it also damages the reputation of the organization.

Attackers often demand vast amounts of money in for the stolen data or for removing the installed malware. Most of the time the victim organizations choose to negotiate with the hackers although officials from the law enforcement warn against obliging the criminals. But the threat of data loss—quickly followed by declining customer base—is too big to handle.

Researchers have conducted a study of happenings in 2022 focusing on three key areas besides others:

- The number of ransomware incidents in 2022.
- Types of organizations that were targeted.
- Amounts of ransom paid to the hackers.
- And a lot more.

Here are some of the statistics that elucidates the status of ransomware during the period of 2021-2022.

PREVALENCE OF ATTACKS

- The number of ransomware attacks rose to a staggering figure of 188.9 million.
- Ransomware remained one of the most common types of malware because it offers an opportunity to extort large amounts of money without posing any risk to cyber criminals.
- Ransomware was the second leading cause of data breaches. It is only exceeded by phishing.
- More than 623m ransomware attacks worldwide were launched last year. Of these nearly half—about 304m were detected.
- The attacks were mostly launched on systems which operated on Windows and Mac OS. But 146% hike was witnessed in Linux based ransomware attacks.
- An overwhelming majority of organizations—about 76%--experienced one or more attacks during the period. Of those 76%: 42% were cause by unintentional user actions whereas 43% were cause by negligence of managers and administrators.
- 42% were unintentionally caused by user actions, such as clicking on malicious links from spam emails.
- 43% were due to negligence from managers or administrators (risks concerning software patches, credentials, etc.) [Veeam]
- In 2021, hackers successfully encrypted data in 65% of attacks, up from 54% recorded in 2020. [Sophos]
- In 2021, there was an 82% rise in ransomware incidents, with 2,686 attacks as opposed to 1,474 in 2020. [CrowdStrike]
- During the first half of 2022, there were 707 ransomware attempts per organization. [SonicWall]

BATTLEGROUNDS OF ATTACKS

Criminal gangs have a preference to target prosperous countries for their attacks. The United States continues to head the list when it comes to bearing the brunt.

US	— 51%
UK	— 10%
Canada	— 5%

Australia — 3%
France — 3%
Japan — 2.5%
Brazil — 2%
Germany — 2%
Rest of the world — 21%

ORGANIZATIONS SUFFERING ATTACKS

Ransomware attacks rarely discriminate between the various types of businesses or the nature of organization. The attack can be directed towards any organization in any area. However, some pattern was also seen in the choice of business although it may be a mere coincidence.

Sector-wise ransomware stats: Legal 92%, Manufacturing 78%, Financial 78%, Human Resource 77%.

Critical Infrastructures suffering the attack: Of the 16 sector, attacks were launched on 14 sectors including Emergency Services, Food and Agriculture, IT, Government Organizations.

Cost Intensity: More than 86% of the victim organizations reported that the ransomware attacks proved costly and they had to suffer a huge financial burden in the form of ransom payment and for addressing reputational damage.

Rate of Increment in Ransomware: The retail industry was the most affected in the past two years when ransomware attacks demonstrated a 100% increase—the highest in any business. The tech industry was next at 89% while healthcare facilities showed an escalation of 30%.

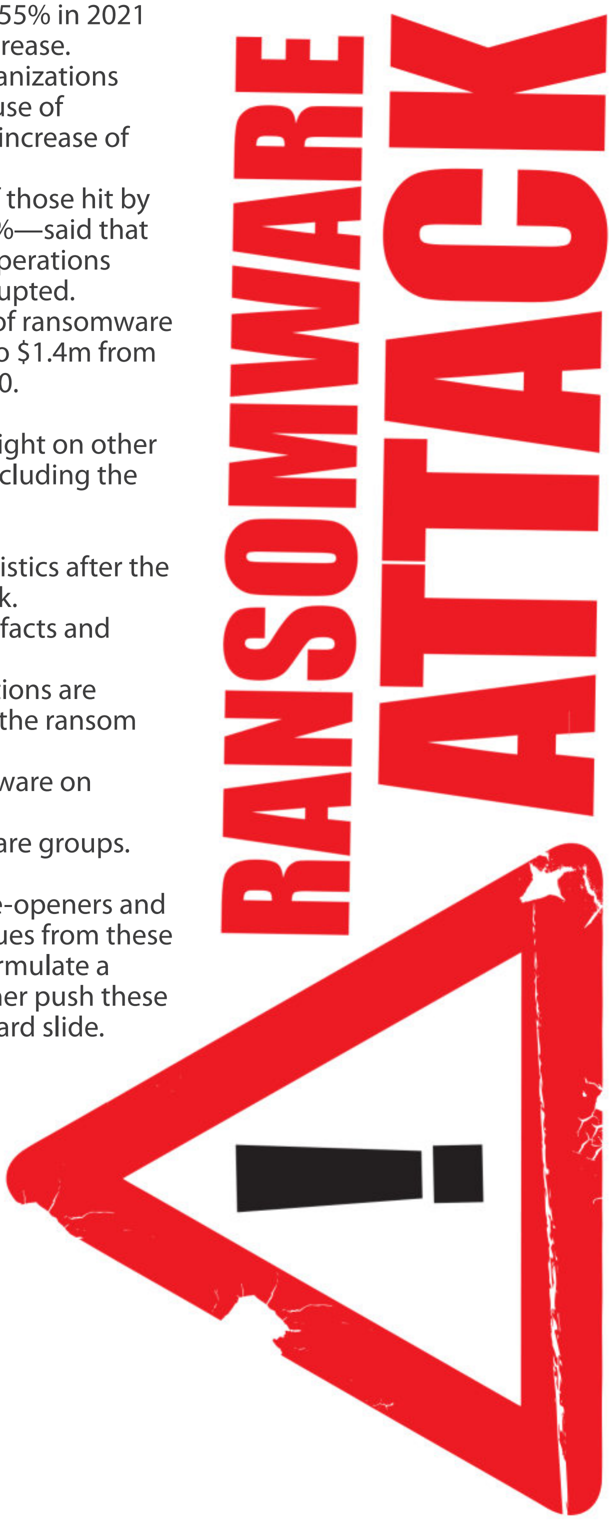
COSTS OF THE CRIME

- There was a dramatic increase in the global costs of ransomware: from $325 million in 2015 to $20 billion in 2021.
- Losses in the range of $1m to $10m were reported by 67% of companies.
- Losses in the range of $25m to $50m were reported by 4% of companies.
- Nearly 37% of businesses had to lay off some of their staff as a result of ransomware attack.
- More than 35% of respondents said their company had to face resignations from c-suite executives.
- Over 33% businesses had to halt their operations—though temporarily—after the attack.
- The percentage of organization attacked by ransomware rose to 73%—up from 55% in 2021 which is a 33% increase.
- About 66% of organizations faced losses because of ransomware—an increase of 78% from 2020.
- A large number of those hit by ransomware—90%—said that their company's operations were severely disrupted.
- The average cost of ransomware attacks dropped to $1.4m from the $1.85m in 2020.

The survey also shed light on other aspects of the affair including the following:

- Data recovery statistics after the ransomware attack.
- Ransom payment facts and figures.
- Reasons organizations are compelled to pay the ransom amounts.
- Impact of ransomware on security budgets.
- Top five ransomware groups.

The statistics were eye-openers and thought leaders get cues from these facts and figures to formulate a strategy that can further push these activities on a downward slide.



Hacked Accounts

Here are ways you can regain control if your account has been compromised or hacked. WHAT ARE SOME SIGNS THAT MY ONLINE ACCOUNT HAS BEEN HACKED?

When hackers strike, acting fast is crucial. But to act fast, you need to determine that one or more of your online accounts has been compromised. Here are some quick tips to see if someone else has gained access to your account: There are posts you never made on your social network page or your account has sent direct messages that you never wrote. Commonly, these posts may encourage your friends to click on a link, download an app, or buy something through an online store.

A friend, family member or colleague tells you that they received emails from your email address that you never sent.

Your information was lost via a data breach, malware infection or lost/stolen device. Companies are required to tell you if your data was compromised in an incident.

DIGINFO®
TRUSTED LEADER IN CYBER SECURITY

DGCLOUD | SECURE CLOUD PLATFORM

WITH CLOUD TECHNOLOGY, YOUR PERFORMANCE— AND BUSINESS—CAN REACH THE SKIES.

DG CLOUD helps customers to define, manage, operate, maintain and have full visibility on their cloud environment.

DG CLOUD is a unique platform that orchestrates the deployment of computer and virtual infrastructure resources and of complex multi-tier application architectures.

It integrates and leverages the strengths of a hybrid cloud environment, providing the ability to design and deploy enterprise-ready services tailored to the business needs of your organization.

DG CLOUD PRODUCTS

DG CLOUD Workplace

DG CLOUD Workplace is a fully automated virtual office with all necessary virtual servers: configured and ready to use.

DG CLOUD DevOps

DG CLOUD DevOps provides full, ready-to-use infrastructure for Cloud Based Collaborative Software Development.

DG CLOUD Sparks

DG CLOUD Sparks provides high end servers for dedicated tasks with dedicated computing resources for customers.

DG CLOUD Hosting

DG CLOUD provides robust, reliable and secure infrastructure for ERP, In-House Software, SAAS Applications.

dgcloud.diginfo.net

Asif Iqbal
Chief Information Security Officer
MCB Islamic Bank Ltd.

Cybersecurity Warrior

who knows the business inside out

My name is Asif Iqbal and, currently, I am working with MCB Islamic Bank in the capacity of Chief Information Security Officer (CISO) since Nov 2019. My main responsibilities include Information Security Governance, Information Security Risk Management and Cyber Security Awareness.

Previously, I was working with Bank of Khyber, Shaheen Air International, Burj Bank and National Computer Incorporation (NCInc) in different areas that were related to IT infrastructure, data center design, project management and Information Security.

I am very open about myself and like to share that I never waste an opportunity. I started my career as a teacher and then moved into a software house as assistant software developer. Later, due to limited software development, opportunity and work, I decided to move into system administration as system support engineer and there is no looking back.

I have always been an avid reader, and consider myself to be a go-getter when it comes to discovering new things. My technical skills have taken a leap, and the reason is I am a lifelong learner who is always willing to learn something new.

Q&A QUESTIONS & ANSWERS

As you are aware that cyber threats are everywhere in the world and no body or organization is safe, what is your opinion in this regard?

Cyber threats are everywhere and are rapidly increasing around the globe. The cost of cyber crimes has increased to 6 trillion dollars annually making them the world's 3rd largest economy after US and China. The digital transformation around the globe has added to this surge in cyber crimes.
If you look at the global threat landscape, following are the biggest cybersecurity challenges in 2022:

1. Supply chain attacks are on the rise.
2. The cyber pandemic continues.
3. Cloud services are primary targets.
4. Ransomware attacks are on the rise.
5. Mobile devices introduce new security risks.
6. The next biggest threats would be arising from the IOTs (Internet of things).

If we would like to know your enemies, who would you name in a cyber attack? And why is it necessary to protect from cyber threats?

In the murky moral universe of hackers, the line between good and evil intentions is often blurred. But the more we understand about the different types of hackers, their motives and their tactics, the better we can prepare for and prevent future attacks. It's true that some hackers are motivated by ethical or activist considerations, while state backed hacking campaigns aren't motivated by profit. They operate legally in their countries of origin; their purpose is to protect national security interests (including espionage and the propagation of fake news). As such they're often resourced directly by governments. But let's be clear: cybercrime is a vast, multi-billion-dollar industry and businesses need to get a firm grasp on it if they have any hope of preventing future attacks.

Without an effective cybersecurity program and continuous awareness, your organization cannot defend itself against data breach campaigns, which make an irresistible target for cybercriminals. Lack of focus on cybersecurity can damage your business in a range of ways including:

Economic Costs
Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems.

Reputational Cost
Loss of consumer trust, loss of current and future customers to competitors.

Regulatory Costs
GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes.

What cybersecurity measures have you introduced and implemented in your company?

The defense of any organization against cyber threats depends upon the robustness and effectiveness of their cybersecurity posture which comprises People, Process and Technology. The bank has implemented a comprehensive, layered security posture with controls like Next generation firewalls, Web & Email security gateways at the Perimeter, Controls like Endpoint Protection, SIEM (Security Information and Event Management), DAM (Database Access Management), MFA (Multifactor Authentication), Endpoint Detection & Response and File Integrity Manager are at the Endpoints. Privilege Access management and Multifactor Authentication solutions are in place for access control and monitoring / tracking of administrative activities. Apart from these controls on Information assets, the bank has established 24/7 Security Operations Center for monitoring and management of cyber security incidents. The bank has a roadmap to achieved PCI DSS certification in 2023 for the strong processes and controls over cardholder data. We have recently formulated a cybersecurity awareness program and have plans to conduct this program for our staff and customers through a knowledge-based cloud platform as 'People' is the weakest link in the chain of cybersecurity.

How would we tackle non-state actors—black hat hackers?

Dealing with non-state actors in cyberspace is a challenge for states experiencing large-scale cyber attacks launched by such elements. Especially since more and more state actors seem to be hiding behind so-called independently operating non-state actors, it is important to get more clarity on how states could respond to such actors.

To protect the Organization's Information Assets from these threat actors, I would again lay emphasis on developing and implementing an effective and layered security posture strengthening your People, Process and Technology.

How do black hat hackers damage the system?

Black hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage or steals passwords, Debit /Credit card numbers and other personal information. These threat actors typically engage in cyber crime operations and use hacking for financial gain, cyber espionage purposes or other malicious motives.

While hacking might have become a major intelligence gathering tool for governments, it's still more common for Black Hats to work alone or with organized criminals for easy money. The WannaCry ransomware released in May 2017 is one example. Within the first two weeks of its release, it infected approximately 400,000 computers in 150 countries. Fortunately, security experts released decryption tools within days of WannaCry's appearance and their fast response time limited extortion payments to about $120,000.

Do you have all the information that needs to oversee cyber risk?

The main responsibility of the CISO is to provide maximum visibility to the organization in terms of its threat landscape. This is a continuous process and one cannot be sure about having complete information or visibility to oversee cyber risk.

Here Cyber Threat Intelligence (CTI) plays an important part with relevant intelligence to the country and especially the financial sector to manage cyber risk.

Following are some key factors for managing Cyber Risk effectively

1. Information Classification.
2. Identification of Critical Assets.
3. Monitor the risk environment.
4. Monitor data assets.
5. Proper understanding of Roles and Responsibilities.
6. Implement an Incident response plan.
7. Gain management support.
8. Third Party / vendor Risk Management.
9. Build strong external relationships.
10. Enforce security protocols.
11. Evolve with the technological environment.
12. Ensure you comply with the relevant regulations.
13. Invest in Security Awareness.

How effective is your cybersecurity strategy at addressing business risks?

While developing cybersecurity strategy for the bank we had two considerations in mind. Firstly, we conducted a gap analysis of what is missing in terms of People, Process and Technology benchmarking international standards, regulatory requirement, bank risk appetite and

Industry best practices. Secondly, the strategy had to be aligned with our business goals and objectives. Finally, a comprehensive strategy was an outcome both with short-medium term and long-term specific goals.

This whole process ensured that nothing was left out and provided complete visibility of what was required at addressing business risk. We believe that we have made a rightful strategic plan which is effectively meeting business requirements against security risks.

How do we protect sensitive information handled and stored by third party vendors?

In today's interconnected economy, companies rely on third-parties. It's increasingly common to outsource some parts of your business to vendors who specialize in that function, whether that be via a SaaS vendor, third-party service provider or contractor. These third parties aren't typically under your organization's control and it's unlikely that they provide complete transparency into their information security controls. Some vendors can have robust security standards and good risk management practices, while others may not. Some best practices for third party Risk Management include:

1. Adequate due diligence should be performed during the Vendor Onboarding process.

2. Make a practice of incorporating cyber risk into your Vendor Risk Management Program and vendor contracts.
3. Keep an Inventory of Your InUse Vendors so as to understand who all your third-parties are and how much is being shared with each of them.
4. Continuously Monitor Vendors for Security Risks by monitoring their security controls overtime.
5. Collaborate With Your Vendors to reduce risk and fix security issues quickly.
6. Talk About Third-Party Risk by having Leadership engagement on both the sides.
7. Cut Ties with Bad Vendors – the ones with poor cyber hygiene.
8. Measure Fourth party Risk - As important as it is to understand your third-party risk, it's also important to know who your third-parties rely on. These organizations are known as your fourth-party vendors and they introduce fourth-party risk.
9. Follow the Principle of Least Privilege - Many third-party data breaches occur because the third-party is provided with more access than they need to do their job.

Do you have the right data governance strategy to minimize cyber risk?

Yes, we have a Data Governance structure in place and a strategy to minimize cyber risk.

Are your employees fully equipped with cyber technology and have all required certifications?

Yes, our team is well equipped with the latest cyber technologies and the required certifications. Here, I would like to make a point that with high turnover of cybersecurity resources, you need to have a hybrid model which includes your organization's staff combined with vendor outsourcing for relevant skillset and areas. This way you can effectively manage HR needs. We have staff certifications including C-CISO, CHFI, PMP, CEH, CISA, SOC Analyst etc.

What do you think is the biggest cybersecurity threat right now, especially in perspective of Pakistan and what do you suggest to tackle these threats?

Globally, the continued combined impact of the COVID-19 pandemic, socio-political upheavals and ongoing financial stress is likely to increase the number of careless mistakes that employees make at work, creating more exploitable opportunities for cybercriminals.

However, following are the biggest cyber security threats especially in the perspective of Pakistan

- Poor Cyber Hygiene
- Mobile Device Vulnerabilities
- Ransomware
- Poor Data Management
- Inadequate Post-Attack Procedures
- Configuration Mistakes
- User Access Review

Recently some of our government organizations fell victims to cyber attacks. We need to considerably improve the cyber health of the government sector. Following measures should be adopted to counter these cyber threats:

Information Security Governance structure should be improved.

- Timely updatIng of all security systems and software.
- Conducting regular employee cybersecurity training.
- Reducing your attack surface by improving security controls.
- Threat Intelligence feeds relevant to the country.
- Backup and Recover your Data periodically.
- Managing Third Party Risk (Vendors).
- Protecting your physical premises.
- Conducting Cyber Drills & Incident handling trainings.

People receive messages and emails that may be from malicious hackers, how they can be safe?

Banks and other organizations should develop Information Security Awareness Programs and should conduct awareness campaigns to educate their employees and customers on regular basis about the latest and evolving threats.

Do we need cyber security insurance…?

Yes. We need cybersecurity insurance. State Bank of Pakistan has also mandated banks for cyber insurance.

Do you believe that people of Pakistan are well informed about cybersecurity and threats? If they are not well informed please advise?

Cybersecurity is evolving in Pakistan. Cyber attacks and digital frauds are also on the rise as digital transformation is taking place in the country especially in the last two years of the COVID Pandemic. I think people are not well informed about cyber threats as they should be. I believe mass level security awareness campaigns and programs should be conducted through social, print and electronic media to provide awareness to the people.

Please give some suggestions for our viewers to what safe guard they adopt to avoid cyber mishappening?

Here are some best practices that can be followed to avoid cyber mishappenings:

1. Keep Your Software and Systems updated.
2. Implement Security Controls like Firewalls etc.
3. Make Regular Data Backups.
4. Activate Multi-factor Authentication.
5. Ensure Endpoint Protection.
6. Get appropriate Cyber Security Knowledge.
7. Control Access to your Systems.
8. Create Strong Passwords and change them regularly.
9. Secure your Network Devices and Wireless Connections (WIFI).
10. Train Your Staff.

EXPERIENCE SPEAKS LOUDER THAN WORDS

Ransomware Attacks Decrease

OVER 61% DECLINE NOTICED IN 2022

Ransomware is a legitimate risk for anyone having a computer system with data and information as assets. Individuals as well as organizations can be a target of ransomware attack.

In the early part of 2022, the steep incline of 2021 ransomware attacks continued unabated. The attacks ranged from compromising of K-12 student data to disabling of healthcare facilities. But the past twelve months or so have seen a sharp decline in such attacks. Compared to the previous year, fewer people and organizations are paying ransoms.

CensusWide is a global market research company with presence in dozens of countries and bases in in London, Brighton, Scotland and Dubai. The research and surveys they conduct provide 'insight that tells a story.' They conducted a survey sampling more than 300 US based IT decision makers and questioned them about the impact of ransomware on their organizations. The researches shed light on the fact that only 25% of organizations suffered a ransomware attack during 2022. Compared to the previous year, this showed a decline of 61%. During 2021, nearly 64% of organizations admitted to suffering a ransomware attack.

The number of organizations who suffered an attack and paid the ransom also decline from 82% the previous year to 68% at the end of 2022. The decline attests to the fact that organizations and paying heed to the FBI advice to not pay any ransom.

The survey also revealed that hackers prefer to launch attacks on larger companies because of the hefty sum of money they may extract as ransom if the attack succeeds. This is a direct inference from the facts and figures: more than 56% of the ransomware attacks were directed towards companies with 100 or more employees.
With the decline in ransomware attacks, organizations are allocating lesser funds to protect themselves from such attacks. Budget allocations figured at 68% this year as against 93% the previous year.

The number of companies who have incident response plans also declined by a significant margin: 71% from 93%.

Only half of the surveyed organizations are focusing on proactive measures to fight against ransomware attacks. Best practices related to password management are only done by 51% of organization, meanwhile multi-factor authentication is practiced by on 50% of organizations.

Further researches speak of revenue loss by 56%, and lost customers at 50% compared to the figures of previous year. Only 43% of organizations spoke of reputational damage after facing a ransomware attack.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

Spyware, Viruses and Botnets

SPYWARE, VIRUSES AND BOTNETS. THE THREE TYPES OF MALWARE OFTEN USED BY HACKERS.

Malware is short for malicious software. It is a code or file that is intended to harm computers, networks or servers. The first malware was identified as ‘Elk Cloner.’ It was discovered on Apple’s Mac Operating System. The malware on a PC was discovered in 1986 and it was named as ‘Brain.’ Ever since, there has been an avalanche of malicious codes identified by their exotic names and varying types. Spyware, viruses, botnets, root kits, adware, Trojan horses and several others. Cyber criminals liberally deploy such malware to advance their goals. Of these the first three are fairly common.

SPYWARE. Any malware that is deployed without the knowledge or authorization of the end-user can be classified as Spyware. Once installed, the spyware invades the device, steals information including internet data and relays the accumulated data to external users who will find ways to exploit. Hackers deploy spyware to extract credit card numbers, passwords and banking details.

VIRUSES. A computer virus is a type of malware designed to perform destructive activity on a targeted system. The authored code can damage the victim’s file system, steal data, download malware, interrupt online services or can do any other task coded in the malware.
Nine main types of viruses have been identified: Boot Sector Virus, Browser Hijacker, Resident Virus, Web Scripting Virus, Polymorphic Virus, Direct Action Virus, File Infector Virus, Multipartite Virus and Macro Virus.

BOTNETS. A collection of internet-connected devices that are installed with a malware and controlled by an external device is referred to as a botnet. A botnet can be legitimate but often the term is used for a network of computers under control of hackers—their sole purpose being carrying out criminal activity.

Botnets form when a hacker searches for systems with unpatched vulnerabilities that allow for remote control and hacking. When the hacker locates such a system, he installs the malware to initiate a series of destructive steps.

Contact us at +92-21-34325505,
Email : info@diginfo.net | www.diginfo.net

SCAN ME

Cybersecurity News Round-Up

HAPPENINGS IN THE RUN UP TO THE NEW YEAR

The week in August of 2022 was marked by a slew of ransomware attacks in Chile, the Dominican Republic and Argentina. Chile is the most recent victim.
The country's Ministry of Interior reported last week that a government agency had its systems and online services disrupted by a piece of ransomware that targeted Windows and VMware ESXi servers. In the Dominican Republic, the country's national cybersecurity center said on August 24 its Ministry of Agriculture's Dominican Agrarian Institute (IAD) was targeted. It has, so far, refused to pay the $650,000 ransom. Earlier in August, Argentina's Judiciary of Córdoba was struck by ransomware, forcing the organization to shut down systems and services.

The Balkan country of Montenegro has also been struck by ransomware, and the hackers are demanding a massive sum of $10 million. The attack, which was directed at its critical infrastructure, struck on August 19. According to Bleeping Computer, several government spokespeople initially blamed the incident on "Russian services". However, the Cuba ransomware gang has claimed responsibility for the attack.

The Portuguese-state owned airline TAP Air Portugal is the victim of an attack carried out by the Ragner Locker ransomware gang. First disclosed on August 26 the incident appeared to be successfully blocked. The company, at the time, stated it hadn't found any evidence of improper access to customer data. But, on August 31, the Ragnar Locker ransomware gang boasted on their leaks website that the airline's systems were, in fact, breached and that customer data was exfiltrated.

In the United Kingdom, a massive cyberattack against its National Health Service (NHS) continues to wreak havoc since the incident was first announced in early August. This week the NHS announced that some services may be offline for another three months. The attacked has impacted key services, including those used for patient check-ins and medical notes. As a result, some staff have had to rely on pen and paper. It's also likely it will take months to process the increasing amounts of medical paperwork.

NATO is investigating the leak of data reportedly stolen from European missile systems firm, MBDA Missile Systems, which hackers have put up for sale on the Dark Web. According to a recent BBC story the data includes blueprints of weapons being used by NATO allies in the Ukraine War. MBDA Missile Systems has admitted its data was stolen but claims no classified files were part of it. The information was hacked from a compromised external hard drive. The data was leaked for sale on both Russian and English language forums after MBDA refused to pay the ransom of nearly $300,000.

Holders of student loans from Oklahoma Student Loan Authority (OSLA) and EdFinancial got some bad news this week about a data breach via Nelnet Servicing. The breach exposed the data of 2.5 million student loan accounts. The data was exposed after hackers breached technology services provider Nelnet Servicing. The company was breached, which began in June, lasted until July 22. The breach was discovered on August 17.

WARNING FROM BRITISH CYBER AGENCY
RUSSIAN AND IRANIAN GROUPS ATTACKING KEY INSTALLATIONS

British cyber agency popularly known as The U.K. National Cyber Security Centre (NCSC) warned of impending spear-phishing attacks. These attacks are suspected to originate from Russia and Iran and the purpose of these attacks might be information-gathering.
These attacks are state-sponsored, therefore, the general public is not the target. A spokesman for the NCSC said, "The attacks are not aimed at the general public but targets in specified sectors, including academia, defense, government organizations, NGOs, think tanks, as well as politicians, journalists, and activists."

Relentless tracking of the suspicious activities has led researchers at the British spy agency to believe that the groups behind these attacks are SEABORGIUM (aka Callisto, COLDRIVER, and TA446) and APT42 (aka ITG18, TA453, and Yellow Garuda). Their activities carry footprints that are strikingly similar but it is not clear if these two groups are collaborating to launch attacks. The activities show signs of spear-phishing campaigns, where messages are sent to gather information including identity and personal details of the victim. The hackers spend considerable amount of time and exercise immense patience to research the interests of the targeted user which helps them get to the social circles from where some pathway can be found to make a breach.

The initial contact is apparently benign and seems like an attempt to gain trust of the user. The communication can last for weeks, even months, to build confidence until the time when a malicious link is passed on to the user. If he is tempted to click the link, this seemingly small act leads to credential theft and data exfiltration.

The hackers often post fabricated and fake profiles to make their activities appear credible. These profiles impersonate media experts, field professionals, and journalists to coax victims into clicking the malicious links.

According to NCSC , "The stolen credentials are then used to log in to targets' email accounts and access sensitive information, in addition to setting up mail-forwarding rules to maintain continued visibility into victim correspondence."

The Russian group SEABORGIUM is state-sponsored and is active for a number of years. The group has placed fake login pages on the internet which look like login pages of defence organizations and nuclear plants.

APT42 is thought to be the espionage arm of Iran's Islamic Revolutionary Guard Corps (IRGC). It shares overlaps with PHOSPHORUS and it is considered as a part of a larger group identified as Charming Kitten.

The activities of threat actor SEABORGIUM has been under surveillance and it known to operate with fake identities of journalists, researchers, activity groups, and think tanks to get in contact with unsuspecting people. The group constantly changes its tools and arsenal of tactics to remain undetected.

Enterprise security firm Proofpoint, in December 2022, disclosed "The group's use of compromised accounts, malware, and confrontational lures to go after targets with a range of backgrounds from medical researchers to realtors to travel agencies," calling it a deviation from the "expected phishing activity," disclosed Enterprise security firm in December 2022.

A notable aspect of these campaigns is the use of targets' personal email addresses, meant for circumventing security controls put in place on corporate networks. The NCSC director of operations said, "These campaigns by threat actors based in Russia and Iran continue to ruthlessly pursue their targets in an attempt to steal online credentials and compromise potentially sensitive systems."

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

Reporting Cybercrime

The first step toward bringing cybercriminals to justice is reporting cybercrime when it happens.

With just a click of a button on your web browser or an email to IT, you can help take a bite out of cybercrime! But at the end of the day, stopping cybercriminals begins with you. If you are a target of cybercrime, it cannot be rectified unless the authorities are aware of it. This is also true if you were just a potential target of a nefarious attack, like you identified a phishing email or text before clicking any links. Depending on the nature of the attack, reporting a cybercrime can be as simple as selecting a button on your email program.

Remember, you aren't alone online! You have the power to stop cybercriminals!

DG Cyber KIDS.

Empower every child with Cybersecurity know-how

The new scenario, resulting from the pandemic involving work from home and study online has only exacerbated the already increasing incidences of cyber threats. DG Cyber Kids, a product of DIGINFO, provides resources for parents and teachers to educate children as they grow up in a world teeming with technological advancement. The initiative equips children with a sense of cyber safety and ethics. In the process, kids learn more about current terms that have become common like internet safety, bully response, technology balance, digital reputation and privacy.

We are relentless in our mission to improve security—not just for our customers, but for the entire community. We forgo the way information security has been done in the name of better outcomes for all. DG ACADEMY uses practical ways of educating the basics of cybersecurity to children.

DG ACADEMY®

PROTECT YOUR FUTURE