999

SECURITY AND SAFETY FOR ALL

ISSUE 120 JANUARY 2022

FUTURE OF WORK FOR THE UAE'S WORKFORCE

UAE LEADS THE WAY TO A GREEN MIDDLE EAST

IN THE SPOTLIGHT: UAE IN NUMBERS OVER 50 YEARS

HELLO Monday!

UAE CLOCKS IN NEW WORKWEEK

UAE	5.000	AED
KSA	5.000	SAR
Kuwait	0.500	DK
Bahrain	0.500	BD
Oman	0.500	OR

6291100752126

IN THIS ISSUE: *999* CELEBRATES ACTS OF KINDNESS AND COURAGE OF UAE'S EVERYDAY HEROES

STAY CYBER-SAFE IN 2022

THE MODERN INTERNET USERS MUST LEARN TO READ THE BEWILDERING DICTIONARY OF CYBER-CRIME, SO THAT THEY CAN FEND OFF THE 24/7 ATTACKS BEING LAUNCHED BY ONLINE CRIMINALS FROM AROUND THE WORLD

BY ANDREW WILSON

We've arrived in 2022 riding a massive wave of digitalisation, the result of both innovations in technology and precaution during the pandemic. But where there's use of information technology, there's also cyber-crime.

In December 2021, Internet giant Google announced that it had moved to shut down a network of around one million hijacked electronic devices. These were being used globally for committing a variety of cyber-crimes, including user credential theft, and the victims were in places such as the United States, Brazil, India, and South-East Asian nations.

Before that, in November 2021, a blog on the World Economic Forum (WEF) website predicted that cyber-crime trends of 2022 would be related to "deepfakes, cryptocurrencies and misinformation". The writer, Maya Horowitz, who works in the field of threat intelligence and research, said: "The sophistication and scale of cyberattacks will continue to break records and we can expect a huge increase in the number of ransomware and mobile attacks."

In 2020, Dr Mohamed Hamad Al Kuwaiti, Head of Cyber Security - UAE Government, said that there was a 250 per cent increase in cyber-attacks in the UAE, with phishing and ransomware incidents surging. Corporations in the UAE faced over 1.1 million phishing attacks in 2020.

"There is a cyber pandemic, not only a biological pandemic," said Al Kuwaiti at the Gulf Information Security Expo and Conference in Dubai in December 2020. "The financial sector was one of the most attacked areas, as well as the health sector," he added.

> **"There is a cyber pandemic, not only a biological pandemic. The financial sector was one of the most attacked areas, as well as the health sector**

Dr MOHAMED HAMAD AL KUWAITI
Head of Cyber Security,
UAE Government

> **"The sophistication and scale of cyberattacks will continue to break records and we can expect a huge increase in the number of ransomware and mobile attacks**

MAYA HOROWITZ
VP Threat Intelligence & Research,
Check Point Software Technologies

As more and more words are added to the dictionary of cyber-security and cyber-crime, it may appear increasingly confusing to the general Internet user. But our online lives are now as full of risks as our offline lives, and effective risk mitigation begins with knowledge.

For most people, cyber-security is something they've heard about or have seen in news articles on their social media feeds, but they don't think it has anything to do with them. The fact is: cyber-security is relevant to every one of us, if we want to protect our bank balance, our business, our jobs, or the peace of mind of our family members.

Cyber-crimes cost the global economy over $1 trillion (Dhs3.76 trillion) in 2020 with estimates of global losses for 2021 to be much higher, according to cybersecurity firm McAfee. The COVID-19 pandemic has meant misery and problems for most people, but it has been a blessing for cyber-criminals, as it has forced many people to work from home on unsecured computers and networks. Canalys, a private tech market analysis firm, reported that 30 billion data records were stolen in 2020, which was more than in all the previous 15 years put together.

Some of you are thinking how this could affect you. Well, it could be your data and personal details that are in the records being stolen. The pandemic has forced all

of us to use online services much more than we did before. Most people these days have a smartphone, which they use not only for talking with friends but also for shopping, banking, and business.

If a cyber-criminal gets access to your smartphone, think about what personal photos and information they can use to steal your identity.

CASE IN POINT

A rampaging horde of global cyber-criminals is active 24/7. They are just waiting for you to make one mistake with your online lifestyle. Your online security depends on your cyber awareness about the threats in your online activities.

Jemma was an attractive female personal trainer in the United Kingdom who worked hard and built a strong client base. To do this, she had often posted photos of herself working out in the gym and linked them to various social media websites. After a while, Jemma was approached in the streets by several men. She was also starting to have gifts and abusive letters sent to her address; these were from men who wanted to meet her from dating websites. But Jemma had never been on those dating websites.

Eventually, a friend showed Jemma a dating app profile that had been created in her name; this was a 'no strings attached' hook-up app, where people met purely for affairs without emotional commitment. The profile was packed with her gym photos and a bio saying that she was keen to meet local men. Jemma contacted the local police to complain, and a stalking and harassment investigation was launched.

The detective in charge was directed to contact the website owners and request details of who owned the account on their dating site. Unfortunately, the suspect was quite knowledgeable about how the Internet worked, and had enlisted the services of a VPN, short for a Virtual Private Network. Designed to protect your network connection when using public networks, VPNs encrypt your Internet traffic and disguise your online identity.

THE NUMBERS

Dhs3.76 trillion

Amount of losses that the global economy suffered due cyber-crimes in 2020, according to cybersecurity firm McAfee

30 billion

Total number of data records across the globe that were stolen by cyber-criminals in 2020, says Canalys, a private tech market analysis firm

1.1 million

The number of phishing attacks faced by corporations in the UAE in 2020, with a 250 per cent increase in cyber-attacks in the same period, as per Dr Mohamed Hamad Al Kuwaiti, Head of Cyber Security - UAE Government

Matt Trott, who was part of the team that investigated Jemma's case in the United Kingdom, said that they had no credible lines of enquiry, as they found later that the dating website was based overseas and was out of British jurisdiction.

Trott, who has over 30 years of experience within the British police and military as an undercover operations specialist and now provides investigations, security consultancy and training services, told ***999***, "All the police could do in this case was to offer advice around personal safety and to warn against sharing images online. Companies like Google can do reverse image searches and delete unwanted pictures; however, this facility was in its infancy at the time and usually reserved to prevent pornographic images of children being shared online."

Discussing his general police work, Trott said, "As a detective sergeant, I had to supervise investigations and had to set an investigative strategy for my detectives to follow. By far the hardest of these investigations would have been cyber-crime offences. These come in many formats and include personal crimes like stalking and harassment all the way through to data breaches and malicious damage caused to intellectual property and company records.

"The main difficulties for your standard law enforcement agency are that of capacity, ability and the competing demands of threat, risk, and harm. The average detective has a basic understanding of Internet safety, and a more advanced officer may know how to check your hard drive for malicious software. Beyond that, you have little or no hope of them identifying who has targeted you, or where your data or money has gone."

> **"A more advanced officer may know how to check your hard drive for malicious software. Beyond that, you have little hope of them identifying who has targeted you, or where your data or money has gone**

MATT TROTT
Undercover operations specialist in the United Kingdom

NOTORIOUS HACKER GROUPS IN THE WORLD

LIZARD SQUAD

This group has claimed responsibility for hacks against Facebook users. The group did manage to successfully hack pop star Taylor Swift's Twitter account, and several members of Lizard Squad have been arrested and charged for their activities.

EQUATION GROUP

The cyber-security company Kaspersky first announced its discovery of Equation Group in 2015, calling it "the most advanced" hacking group it had seen to date. In that year, there were around 500 documented malware infections by the group in at least 41 countries, but the actual number could be in the tens of thousands due to its self-terminating protocol.

LAZARUS GROUP

This group was believed to have started in 2009, and mostly uses malware in its attacks. It's responsible for Wannacry, a ransomware software that requires users to pay up to re-access their own data, once the data is held to ransom by the hackers. Lazarus Group has also had a large amount of success with cryptocurrency theft. So far, it has managed to steal $471 million from different cryptocurrency exchanges.

CARBANAK

Very little is known about this mysterious hacking group, but so far it has managed to steal millions from banks. The alleged mastermind behind the group was arrested in 2018 along with two other high-ranking members. However, Carbanak has carried on successfully without them. Some of them were arrested for theft of credit and debit card records from restaurants, casinos, and other businesses across the US, as well as in the UK, France, and Australia, with losses totalling tens of millions of dollars.

ANONYMOUS

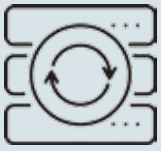
Known for wearing Guy Fawkes masks, the Anonymous group has been behind some of the largest hacks of the 2000s. Anonymous has been involved with hacks related to the Church of Scientology, the Occupy Wall Street movement, the Westboro Baptist Church, and many more.

FAKE HOTSPOTS

This is a very common type of cyber-crime that's easy to fall for. In a fake WAP (Wireless Access Point) attack, the hacker sets up a wireless router with a convincingly legitimate name in a public spot where people might connect to it.

KEYLOGGER ATTACK

In this attack, the hackers record all keys struck on your keyboard with keylogging spyware that can be installed on the target device. While keylogging software is not illegal and can be bought commercially, it can be used for illegal activities.



CREDENTIAL REUSE

This attack follows a data breach for a server hosting many users' login information. The hackers use the stolen data, such as people's passwords and information, to log into social media, banking or business sites and networks.

THE DARK WEB

It's a fact that computer networks are under constant attack from cyber-criminals. Whereas many years ago, organised crime would use thugs and violence to steal and extort money from honest citizens, now they use hackers who give them a global reach.

It would be impossible to list all the cyber-attacks and data breaches, as they're happening constantly. Criminals have been stealing data and financial records, but a darker side is where they target a country's critical infrastructure, such as power grids, medical, public safety or security organisations.

To contextualise this, in February 2021, a group of hackers tried to poison the water supply for a city in Florida, United States. An outdated version of Microsoft Windows and a weak cyber-security network allowed hackers to access a wastewater treatment plant's computer system and tamper with the water supply. The hackers attempted to change the water supply's levels of sodium hydroxide. At high levels, sodium hydroxide severely damages any human tissue it touches.

Luckily, the person monitoring the water supply system noticed that his mouse cursor was moving strangely on his computer screen and out of his control. Initially, he was not concerned, but when he saw that the levels of sodium hydroxide being added to the water had been increased, he realised there was a problem and reported the incident. Investigations were then taken up by the police, FBI, and US Secret Service. No one is sure who the hackers were or from which country the attack originated.

COMMON TYPES OF HACKING

BAIT AND SWITCH

A bait-and-switch attack uses fake ads to fool people into visiting malicious websites. Once the person has clicked on the ad, the attacker can use a number of other attacks, like downloading malware, clickjacking, or browser locking, to compromise the user's system.

BRUTE FORCE ATTACK

In a brute force attack, the hacker uses a trial-and-error to guess passwords, PINs, or encryption keys. Hackers will employ software that will run multiple password combinations per second till they find a correct password.

MACRO MALWARE IN DOCUMENTS

Many document types, like .doc or .pdf, can run scripts when opened. These functions usually have to be permitted by the user to run through a prompt when the document is opened. If you give the document permission to run the macro malware, you will open numerous vulnerabilities in your system, allowing hackers to upload more serious malware and take control of your computer.

DDOS ATTACKS

DDoS (Distributed Denial of Service) attacks use malware installed on a target's device to perform an attack, but don't really hurt the device infected by it. The hackers turn the infected device into part of an army of bots that the hacker can use to completely flood their target with fraudulent requests and shut their server down.

PHISHING

Phishing attacks target the person behind the device, rather than the device, and is one of the most popular hacking tactics. By tricking the user through a convincing e-mail or other messages, the hacker convinces or scares the user into providing access to their most sensitive information, opening a malicious URL or malware-infected document.

HOW HACKERS ATTACK

Hackers use a wide variety of tactics to attack their targets; as long as you're using the Internet with a computer or a smartphone, you can become a victim of hackers. People fall victim to hackers through social engineering or phishing attacks; by visiting dangerous websites; by using malicious USB sticks; using weak passwords; or causing BYOD ("Bring Your Own Doom") incidents.

BYOD is where people log onto their work networks with their personal and unsecured devices. This type of attack has boomed since the COVID-19 pandemic and the widespread adoption of the work-from-home (WFH) model. Also, network hacking, web app attacks, and attacks on vulnerable applications are very common.

The use of ransomware is a major tactic used by cyber-criminals. Ransomware is a type of malware that prevents users from accessing their network and data, either by locking their screen or by locking the users' files until a ransom is paid. More advanced ransomware encrypts files and data on infected networks and devices, and forces the users to pay the ransom through online payment methods to get a decryption key.

HOW TO PROTECT YOURSELF AGAINST CYBER-CRIMINALS

Here are some basic cyber-security procedures that you should follow. They're not difficult and need to be a regular part of your online security routine.

- Make sure your device software is up-to-date
- Install reputable anti-virus and anti-malware software
- Make sure your security software is kept up-to-date
- Disable online connections when you aren't using them
- Create unique passwords and PINs for all devices
- Only install trusted applications
- Review your network and device names
- Only log on to trusted hotspots and networks
- Use multifactor authentication on your accounts
- Delete suspicious e-mails
- Do not click on suspicious links or download unknown documents
- Be cautious with "Save my information for next time" on public or non-private networks
- Sign up for account alerts

The ransom demanded for the decryption key varies greatly, depending on the hackers and who they're targeting. Ransoms are usually paid in cryptocurrencies, but some criminals have used alternative payment options such as iTunes and Amazon gift cards for smaller ransom amounts. As with all kidnap-and-ransom situations, payment of a ransom does not guarantee that the hostages — in this case, files and data — will be released and the decryption key provided.