ISSUE 02 FEB 2018

إشارات Esharat

Dedicated to a safer cyberspace

HH SHEIKH HAMDAN APPROVES DUBAI FUTURE FOUNDATION'S 2018 PLAN

SURF SAFELY WHILE CONNECTED

THE POWER OF PKI, WITH ENGINEER AFRA BIN FARES

HOW BLOCKCHAIN IS CHANGING THE FUTURE FOR DUBAI

Beware of your own greed!

Research suggests that many cybercrime victims fall prey to their own greed. If you receive an email or a message promising money or reward in return for what seems like very little, remember this:

- If it sounds too good to be true, it probably is.
- Be extra vigilant, ensure you know what you are clicking on.
- Spread the message among those you know.

STAY SAFE

DUBAI ELECTRONIC SECURITY CENTER

A magazine specialised in cyber security and technology, issued by Dubai Electronic Security Center

Director General
Yousuf Hamad Al Shaibani

Managing Editor
Amer Sharaf

Editorial Secretary
Shaikha Essa
Maitha Khalid

Editorial and Design
7G MEDIA

Editorial Board
Amani Abuseedo
Dan Charter
Ahmed Mersal
Nicole Rehbane

Design and Production
Sree E S
Aws Rahhal

Illustrator
Brian Reyes
Joseph Cartaño

To contact the magazine:
DESC: +971 4 251 2538
7G Media: +971 4 449 5427
info@desc.gov.ae
info@7gmedia.com

INSIDE

A significant milestone

Dubai Electronic Security Center's Memorandum of Understanding with the Smart Dubai Office is a huge milestone for Dubai's transformation into a smart city. The agreement was signed in the presence of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE, and Ruler of Dubai, His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, and Chairman of the Executive Council, and His Highness Sheikh Maktoum bin Mohammed bin Rashid Al Maktoum, Deputy Ruler of Dubai - by Her Excellency Dr Aisha bin Bishr, Director General of the Smart Dubai Office, and myself. This gives an indication of just how significant this partnership is to the future of Dubai.

At its core, this agreement relates to safeguarding Dubai's Digital Wealth and to issuing Dubai Digital Certificates. The Digital Wealth aspect involves the management of the entirety of the digital ecosystem. This includes data and data-storage such as cloud computing, procedures, equipment and software designed to collect and process information, the smart-tech transformation, digital signature and digital ID, paperless transaction management and systems (which includes Blockchain) and smart living in Dubai.

The Dubai Digital Wealth Initiative will help safeguard more than 1,100 smart services and 121 smart initiatives, which is expected to generate AED 33.8 billion in three years.

Smart Dubai and DESC will secure this Digital Wealth and will take responsibility for issuing Digital Certificates to those undertaking the aforementioned smart city projects that will take Dubai into the future.

We will see the level of digital security of all smart services in Dubai increase as work is done to equip the digital infrastructure of Dubai for the future – where we aim to become the most advanced smart city in the world. The Memorandum of Understanding will also ensure that service providers to both the government and private sectors are able to provide their solutions continuously and at the highest level, which in turn meets one of the objectives for DESC set out in the Dubai Cyber Security Strategy.

This agreement is an integral component of the Dubai Digital Wealth Initiative and the Internet of Things Strategy, and it will meet the directives laid forth by His Highness Sheikh Mohammed bin Rashid to implement Dubai Digital Certificates, which will be a predominant factor in maintaining the security and safety of our data and overall digital wealth. We now move forward in a collaborative partnership to transform Dubai into the digital world's smartest, and most secure city.

Yousuf Hamad Al Shaibani
Director General
Dubai Electronic Security Center

Sheikh Mohammed Al Maktoum oversees MoU signing between DESC and Smart Dubai Office to protect Dubai Digital Wealth

> Our push to build the future today has helped establish a digital infrastructure that is now a strategic national asset
>
> **Mohammed bin Rashid Al Maktoum**

His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, and His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai and Chairman of The Executive Council of Dubai, and His Highness Sheikh Maktoum bin Mohammed bin Rashid Al Maktoum, Deputy Ruler of Dubai, attended the signature of a Memorandum of Understanding (MoU) between Dubai Electronic Security Center (DESC) and Smart Dubai Office (SDO), to protect Dubai's Digital Wealth. For the first time in the UAE, the MoU was signed and verified electronically using Public Key Infrastructure (PKI).

The MoU was signed by His Excellency Yousuf Al Shaibani, Director General of DESC, and Her Excellency Dr Aisha Butti bin Bishr, Director General of the Smart Dubai Office and includes the implementation of Dubai's Public Key Infrastructure (PKI) to provide authoritative security to SDO's numerous forthcoming initiatives.

The signing took place at the launch event for the Digital Wealth Initiative and the Internet of Things (IoT) Strategy, which heralded the beginning of Dubai's apparent transformation into a Smart City. In the long term, this is where data will be available in real time, collected and collated to enable citizens with a smarter living experience.

"Dubai's push to build the future today has helped establish a digital infrastructure that is now a strategic national asset in the wake of the Fourth Industrial Revolution," HH Sheikh Mohammed bin Rashid Al Maktoum said.

"The Dubai Digital Certificates and the Dubai IoT Strategy mark the official launch of smart living in the emirate," HH Sheikh Mohammed bin Rashid Al Maktoum continued, "We have directed all government institutions to co-operate and fully implement the initiatives by the year 2021."

DESC Director General, Yousuf Hamad Al Shaibani, said, "Our close cooperation with Smart Dubai provides us with the support we need to fend off cyber-threats and make Dubai the smartest and most secure city from a digital standpoint. Exchanging knowledge and expertise is essential for joint projects, as it enables the participating entities to secure their systems and remain in line with the highest international standards, as well as Dubai's cybersecurity requirements."

Dr Aisha Butti bin Bishr is leading the push towards smart living in Dubai, and one of the first initiatives has just launched, named Dubai Crowd. This is used to visualise large amounts of people and their movements across the city, particularly for large events where decision makers require eyes on the ground to make informed choices on crowd control. "When we launched Smart Dubai in 2014, we sought to enable people to make use of the vast amounts of data generated every day in one of the busiest cities in the world," she said. "Today, as we launch the Dubai IoT Strategy, we provide the people of Dubai with an unmatched smart lifestyle."

IoT involves the linking of every device we come into contact with each day, such as lights, weather sensors, traffic sensors, smart metres, buses and trains. The data collected makes up a large part of Dubai's digital wealth, and DESC and SDO will collaborate to secure this data and digital wealth, while also being able to issue Digital Certificates for smart city projects, setting cybersecurity guidelines and requirements. The MoU is regarded as an important step for Dubai, as DESC is to oversee cybersecurity of all smart services and data, as well as set cybersecurity guidelines and requirements, while regulating the issuance of digital certificates.

"The landmark Dubai Digital Wealth initiative, launched by Vice President and Prime Minister of the UAE and Ruler of Dubai, HH Sheikh Mohammed bin Rashid Al Maktoum, marks the beginning of a new and historic phase in Smart Dubai's mission," Dr Aisha Butti bin Bishr continued.

> We have directed all government institutions to fully implement Dubai Digital Certificates by the year 2021 to protect Dubai's Digital Wealth
>
> **Mohammed bin Rashid Al Maktoum**

"This agreement we've signed is fundamental to implementing His Highness' directives to make the Dubai Digital Certificates a foremost tool in maintaining data security and digital wealth in the emirate, which, in turn, is one of the most important tenets of Smart Dubai's strategic plans to spearhead the emirate's smart transformation. The seamless and secure flow of information is the bedrock on which all smart-tech strategies are based. This partnership with Dubai Electronic Security Center amplifies our cybersecurity efforts and allows us to better identify and address challenges, as well as propose solutions."

The MoU predicates the exchange of information pertaining to common interests, as well as the undertaking of joint projects and regulating the use of published information derived from IoT, Blockchain, Artificial Intelligence, Big Data and other emerging technology.

HH Sheikh Hamdan approves Dubai Future Foundation's 2018 plan

His Highness Sheikh Hamdan bin Mohammed Al Maktoum, Crown Prince of Dubai and Chairman of the Executive Council of Dubai, approves Dubai Future Foundation's 2018 Plan

Hamdan bin Mohammed: Dubai is a future-oriented city and a hub for science

Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, Chairman of the Executive Council of Dubai and Chairman of the Board of Trustees of the Dubai Future Foundation (DFF), said that the emirate is not only taking the lead in shaping the future, but its accomplishments in this domain are also enabling it to export its expertise to the world.

Sheikh Hamdan stressed the importance of staying committed to achieving progress in this field and enhancing efforts to deploy the latest strategies and technology in the government sector to realise the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, to transform the emirate into a future-oriented city and a global hub for advanced science and technology.

Sheikh Hamdan's remarks came at a meeting of the DFF's Executive Committee. At the meeting, he approved the foundation's plans and strategies for 2018 in the presence of Sheikh Maktoum bin Mohammed bin Rashid Al Maktoum, Deputy Ruler of Dubai, and His Excellency Mohammed Abdullah Al Gergawi, Minister of Cabinet Affairs and the Future and Vice-Chairman of the board of trustees and managing director of the DFF.

Hamdan bin Mohammed attends closing ceremony of 3rd Dubai Future Accelerators Program

Crown Prince of Dubai and Chairman of the Board of Trustees for the Dubai Future Foundation (DFF), His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum said that the wise vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, is rapidly leading Dubai to become a model for what a future city looks like, through exceptional and creative solutions for the different challenges.

His Highness' remarks came as he visited DFF headquarters and witnessed the signing of various memorandum of understanding between government entities and a number of prominent international organisations participating in the third session of Dubai Future Accelerators (DFA).

Sheikh Hamdan commended the results of the third edition of DFA, which assert that Dubai is heading to the future through preparing the conducive environment to achieve its objectives. He also said that it focused on developing creative and effective services across various sectors to serve people's lives and enhance their happiness.

His Highness praised the role played by Dubai Future Foundation, which has developed and enhanced the concept of accelerators, to enable authorities to implement the directives of the leadership to speed up the pace of achievement by forming effective joint teams that adopt a scientific perspective and apply future practices; this will provide the world with innovative achievements and creative solutions to create a better future for future generations.

Hamdan bin Mohammed meets with co-founder of Google

HH Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum met with Sergey Brin, Co-Founder of Google and President of Alphabet Inc., Google's parent company.

Sheikh Hamdan praised Brin's knowledge and scientific journey, which is crowned with international success. "Sergey's story is inspiring, as he and his friend, Larry Page, founded Google from a dorm room and then a rented garage when they were in their twenties. Today, the company is worth over US$ 600 billion," he said.

"Sergey's and Larry's story is inspiring, just like Dubai's story. We all share a passion to build the future. They created the future of human knowledge while we created a city that represents the future of urbanism and services for the other cities of the world," Sheikh Hamdan added.

He also stressed that the goal of Google - to organise human knowledge and make it widely available - is inspiring and humane, and that by partnering and co-operating with the company, everyone can make a difference to humanity for decades to come.

With the attendance of His Excellency Mohammed bin Abdullah Al Gergawi, Sheikh Hamdan and Brin explained the potential for co-operation with Google through joint projects that aim to harness the latest information technology and develop the electronic information space, to serve humanity in all areas.

"Dubai aims to become the largest international laboratory to test future technology. Dubai has advanced towards the future, due to the vision of the Vice President, Prime Minister and Ruler of Dubai, His Highness Sheikh Mohammed bin Rashid Al Maktoum, who realised the importance of building a society based on the knowledge economy and constructive investment in science and scientists, as well as connecting modern development with advanced technology," Sheikh Hamdan further added.

He also noted the importance of building strategic relations with international companies. "Developing mutual relations with major international companies is important to developing relations with major countries," he stated.

In the Spotlight

Digital certificates are a crucial component of Dubai's move towards its goal of becoming the safest city in the world digitally

Afra bin Fares

Government entities are shifting from traditional to smart, and transactions are shifting from paper to electronic. According to the latest statistics, the average use of e-government services in Dubai is about 80% of the total volume of transactions with government entities. To address electronic risks and challenges, the Government of Dubai has launched digital certificates to preserve its digital wealth.

Afra bin Fares is a young professional with big ambitions to serve in the Electronic Security Sector as a Researcher at Dubai Electronic Security Center (DESC). Esharat spoke with Afra to find out more about what Digital Certificates are, the concepts behind them, and the positive impact they will have on Dubai.

Afra is responsible for the management of the Public Key Infrastructure (PKI) leading a specialised team in the implementation of this project for the Dubai government.

She explained to Esharat: "First, I would like to define digital certificates, outline their importance and clarify their role in the digital world. At the most basic level, digital certificates aim to prove and verify the identity of users in the digital world. In real life, an individual's identity can be verified by checking his ID as validation to ensure he's not impersonating someone else. In the digital world, digital certificates play that role - they verify the identity of online clients."

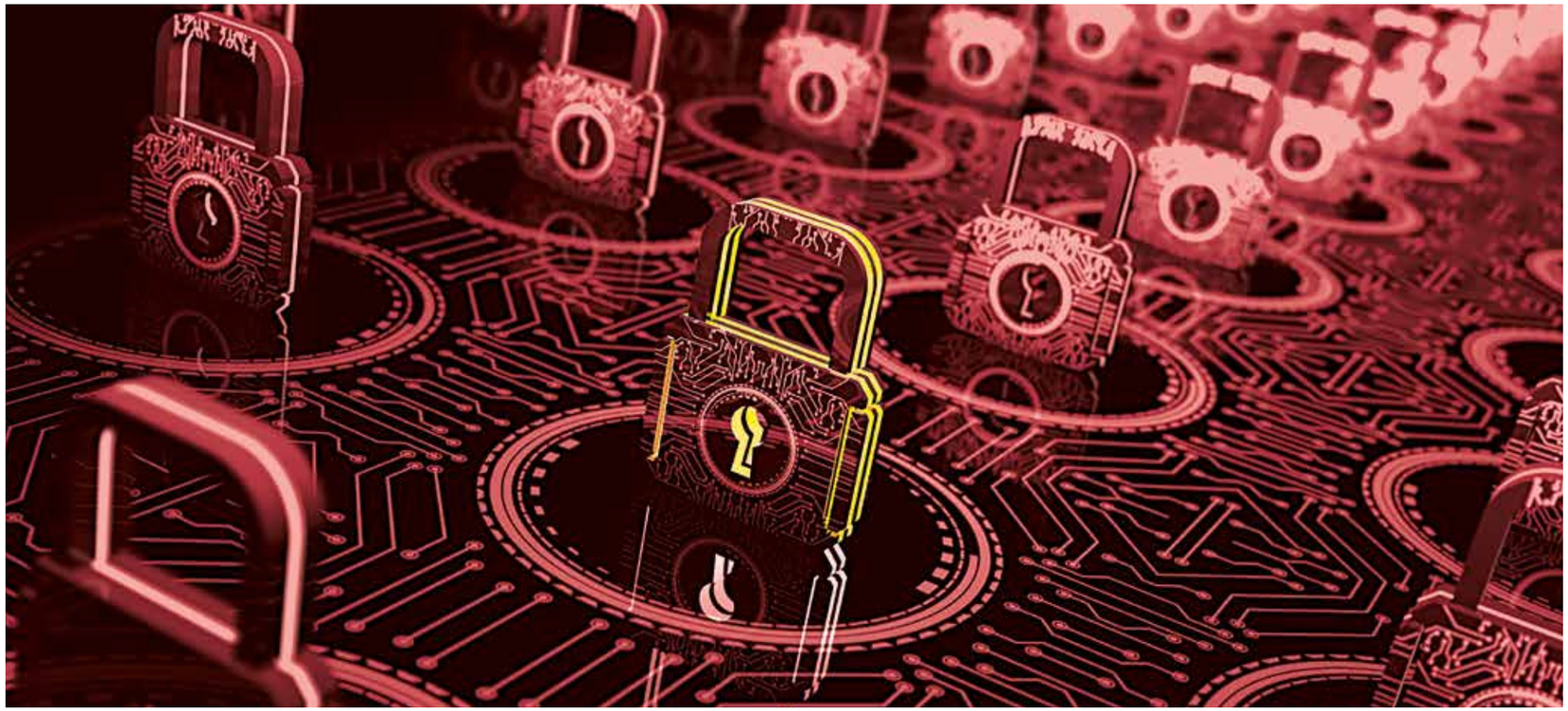
Furthermore, Dubai Digital Certificates can verify the identity of an organisation or company. For that reason, they establish online trust between different parties. At this stage, Dubai Digital Certificates are aiming to enable government and semi-government entities and institutions to provide their services or products to users with complete security.

The project is in line with the directives of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, and His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, that all government entities in the emirate will cooperate to preserve the digital wealth of Dubai.

His Highness Sheikh Hamdan confirmed that the dual initiatives of Dubai Digital Certificates and the Internet of Things support our full readiness for a paperless government by 2021. He also directed government entities in Dubai to make digital certificates an integral part of their work. All that will help make

> "The digital certificates are used to encrypt online data and information, and these certificates ensure confidentiality"

In the Spotlight



> Digital certificates enhance the credibility of organisations as well as the trust amongst their online clients

Dubai the smartest city in the world. He explained that having a more digitally sophisticated city will enhance the level of satisfaction and happiness of its residents. It will open up new horizons for upgrading efficiency and productivity in various work sectors in Dubai."

Ensuring Security in Information Exchange

Regarding the ability of digital certificates to ensure information security along with verifying the identity of the users, Afra said: "Dubai Digital Certificates ensure the security of all the data exchanged between parties. The digital certificates are used to encrypt online data and information, and these certificates ensure confidentiality."

The Infrastructure

On the topic of infrastructure, Afra continued: "A standard digital certificate will consist of hardware and software, plus a range of policies and standards to ensure it operates responsibly and according to the best international practices. In implementing the system, we have benchmarked a selection of European Digital Certificates and followed the WebTrust principles and criteria, which are designed to promote confidence and trust between entities and companies conducting business on the Internet. Through that process, we've ensured we are meeting the highest standards."

"By turning to the experience of several developed countries in this field and building upon them, we've created an advanced version of digital certificates suitable for the needs of Dubai and the projects we have," she said.

"At DESC, we are confident that digital certificates will have an enormous impact on Dubai in terms of online security, which is required for many of the projects in the pipeline at the government level. Digital certificates are a critical element of the process and of our progression in Dubai to becoming a smart city at the top of technological advancement; they are also essential in protecting Dubai's digital wealth."

Developing Immunity Against Digital Piracy

"The Dubai Digital Certificates are designed to completely eliminate the threat of hacking through certificate abuse with government entities," Afra clarified, "Our digital certificates add an additional layer of security, that means hackers and cyber criminals cannot commit fraud, or assume a false identity online."

"With Dubai's plans to launch pioneering projects to achieve the Smart City concept, digital certification has become the basis of a solid foundation of security and electronic integration," Afra said.

"Implementing digital certificates will mean the security level of Dubai will correlate with its ambitions in the technological sector. All the projects that Dubai departments are looking to launch depend heavily on digital certificates," Afra explained. "For instance, many of the projects that the Smart Dubai Office is currently working on—such as Blockchain or the IoT platform—are unique projects that are enabled through digital certificates."

Smart Solutions Come with Higher Security

"We started working on Digital Certificates in May 2016, and they will soon be introduced for government use. We are now well into finalising the infrastructure, which is an advanced stage of the project," Afra said.

"We expect that Dubai Digital Certificates will be up and running by beginning of 2018, and the DESC will introduce it to the Dubai Government to be adopted by all its entities," she further added.

> The Dubai Digital Certificate deals with cyber criminals who are a threat to government entities

"As the Digital Certificates prepares to launch, it represents another key step for DESC in fulfilling their strategy and their mission to make Dubai the safest city in cyberspace. I look forward to working with the team to achieve the vision of the emirate of Dubai established by His Highness Sheikh Mohammed bin Rashid Al Maktoum. We aim to implement the directives of His Highness on digital transformation to make Dubai the smartest city in the world."

"Although the Dubai Digital Certificates is an ambitious project filled with technical challenges, we have been able to achieve our goals within record time. With the rapidly changing technology sector around the world, each day we face new challenges. Therefore, in Dubai, we have adopted a proactive approach in leading technology rather than wait for what the future brings," she concluded.

DESC signs MoU with Institute of Electrical and Electronics Engineers

In the spirit of furthering its cooperation and ties with other UAE entities to disseminate science and knowledge in the country, DESC has signed a Memorandum of Understanding (MoU) with the Institute of Electrical and Electronics Engineers (IEEE) UAE section. The MoU was signed by His Excellency Yousuf Hamad Al Shaibani, Director General of DESC, and Dr Essa Basaeed, IEEE UAE Section Chair, in support of Dubai's Cyber Security Strategy, which includes the need for innovation, knowledge dissemination and the promotion of research.

Both DESC and the IEEE acknowledged the signing of the MoU signifies the dawn of a new era for the two parties that will see a number of joint initiatives launched that will raise awareness of cybersecurity issues among the public. The intent is to host international events, to embark upon initiatives that support corporate social responsibility and to hold training courses, workshops and conferences.

The MoU strengthens the level of cooperation between DESC and the IEEE, and one of the outcomes will be the development of new and upgraded educational materials and programmes on information security.

In a statement made at the signing, HE Yousuf Hamad Al Shaibani said: "Building a free and innovative cyberspace will only be achieved by supporting research projects and scientific conferences."

On behalf of his organisation, Dr Basaeed said that IEEE is committed to making a great contribution to UAE society. "Our collaboration with DESC to organise various activities in the field of cybersecurity reflects our commitment, at the IEEE UAE Section, towards contributing to our society," he said.

Dubai Cyber Security Strategy Website Launches

The official website of the Dubai Cyber Security Strategy has been launched by DESC. The website, which comes soon after the official unveiling of the strategy by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, is a sophisticated and customised website that contains simple to understand text with infographics and a unique design to resonate with the residents of Dubai.

Contained within the website are the five domains of the strategy: Cyber Smart Society, Innovation, Cyber Security, Cyber Resilience, and (Inter) National Collaboration, as well as a timeline that marks out the journey towards completion of the strategy.

The newly-launched website can be found at *desc.dubai.ae*.

DESC organises Dubai Cyber Security Strategy KPIs workshop for government entities

DESC held its third workshop in support of the implementation of the Dubai Cyber Security Strategy for government entities. The workshop which ran under the heading: "Dubai Cyber Security Strategy KPIs" was attended by government and semi-government bodies, and discussed in detail the key performance indicators, initiatives and other activities that relate to the strategy.

The workshop itself is one of a number planned that meet the objectives set out by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, to have a united front across all government institutions and the private sector in order to provide a secure cyberspace. Discussing the workshop, Amer Sharaf, Director of Compliance Support and Alliances, said that cooperation with governmental and semi-governmental entities is integral to achieving the strategic plan vision.

DESC Dubai Cyber Security Strategy discussed in a workshop with RTA

DESC has teamed up with Dubai's Roads and Transport Authority (RTA) so as the latter can conduct an analysis of the core objectives set forth in the strategy document. The leaders and staff at RTA participated in a workshop to raise awareness of cybersecurity and the strategy implemented by DESC.

Part of DESC's remit is to work alongside Dubai's government entities to disseminate knowledge of the threats that exist online and to lay forth the objectives and key drivers of the cybersecurity strategy. Working alongside large public sector entities, DESC advises on how to prevent unnecessary exposure to risk, providing a shield against cybercriminals for whom the data and information kept by many of Dubai's entities would be of great interest.

Abdullah Al Bastaki, Director of Technology Strategy and Governance, Corporate Technology Support Services Sector, RTA, noted that his organisation has made a huge commitment towards meeting the objectives of the strategy for their part, with the overall goal of contributing towards making Dubai the safest city in cyberspace. "The underlying objective of the Dubai Cyber Security Strategy is to curb cyber risks, tackle cybercrimes, and enable users access to a broad spectrum of IT," he said. "Such objectives can be achieved in five domains namely: Cyber Smart Society, Innovation, Cyber Security, Cyber Resilience, and (Inter) National Collaboration. RTA is committed to making periodical reviews to ensure that all affiliated sectors and agencies comply with the approved standards set by the Dubai Electronic Security Center."

Amer Sharaf, Director of Compliance, Support and Alliances at DESC, said that cooperation with government and semi-government entities is crucial for the implementation and accomplishment of the strategic plan. "The vision of the plan," he said, "is to raise the profile of Dubai as a leading metropolitan city in innovation, safety and security."

How Blockchain is changing the future for Dubai

The introduction of Blockchain in Dubai for a number of applications is already visible, and many more examples are set to be realised as part of the Dubai Blockchain Strategy. Esharat looks at the impact of the Blockchain, and some of the areas in which its effect could be to advance and refine.

> Dubai will continue to evaluate and explore all the possibilities for Blockchain application

Blockchain is, for the most part, associated with cryptocurrency, and certainly for the first few years the ledger component took the back seat while the currency stole the headlines. Now, the possibilities for the application of Blockchain technology in almost every facet of modern government, finance and social concerns, has been fully recognised, especially in Dubai. Currently, Smart Dubai is working towards accomplishing the directives of His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, set out in the Dubai Blockchain Strategy in December 2016.

The strategy states that Smart Dubai, in collaboration with the Dubai Future Foundation will continue to evaluate and explore all the possibilities for Blockchain application in Dubai, to contribute to the target of making the emirate one of the most innovative, technologically advanced, safe, transparent and efficient destinations on the planet. In that regard they have now partnered with IBM and Consensys to help with the city-wide implementation of the technology.

The power of Blockchain in terms of its transparency in finance will have positive impact on the financial sector and the way banks will operate in the future. With the enhancement of safety and security of transactions, as well as accountability, this technology serves as a shield to protect the world from financial crises.

Blockchain has many more uses though, and Dubai Government targets these uses and applications to help it become the world's first Blockchain-powered government, positioning it at the head of the world's future economy. From the reduction in documentation alone, the overall savings are predicted to be AED 5.5 billion, and the paperless government services aspect looks to be on schedule for its 2021 target.

The improvement of government efficiency is a continual target for Dubai. And Blockchain has the capability to accelerate governmental procedures and have a real impact on public services such as education and healthcare. Blockchain is the solution that aids governments in optimising their efficiency, and also their security, in every area of their work and services.

One of the revolutionary applications has been within healthcare, where MedRec provides a decentralised record management system that uses the Blockchain technology to manage data, confidentiality, accountability and authentication for the entire sector. Its widespread adoption could completely transform international healthcare in every respect.

Dubai Land Department has already become the world's first government entity to conduct all transactions through a Blockchain network in collaboration with Smart Dubai and other partners. Its Blockchain system uses a smart and secure database that records all real estate contracts, linking them with DEWA, telecoms and other bills related to property. The platform contains details of tenants, residency visas and Emirates IDs. It also enables tenants to pay electronically within a few minutes.

It is transactions such as those implemented by the Dubai Land Department that Dubai is targeting across the board for implementation in all government entities by 2020. The more Blockchain is refined and developed, the more applications it has. And despite the attention it has placed upon it right now, Blockchain is still largely undefined and untapped. The exploration stage is still very much in process, and there is undoubtedly much more that can be derived from the technology than just making government transactions more efficient. There are now global teams looking into ways it can be applied to help with humanitarian crises, with assisting third world countries in making transactions, and giving the world access to general information.

The main appeal for the public with regard to Blockchain is the transparency it ushers in. Dubai, with its adoption of open data and its commitment to transparency, will be looking to lead the way in this regard.

> Dubai Land Department became the first government entity to conduct all transactions through Blockchain

Surf safely
Tips for how to stay protected while connected

In 2018, the need to protect yourself and to consider your every online action on a daily basis has never been more vital. While today's environment keeps us connected through the instant sharing of information, who's to say that information isn't being shared upon you at this precise moment? Someone somewhere is probably interested in learning something about you, so how can we protect ourselves to the maximum? Here are some tips to retaining an element of mystery about your online persona, but also to keep yourself safe from the repercussions that can be associated with your online actions.

Connecting to WiFi networks

It is recommended that you only use trusted WiFi connections and avoid those with ambiguous or suspicious names.

If you do use a public network, log off the moment you are done. And never use it for online banking or shopping.

Surfing the web

The Internet is full of inspiring, informative content, but it's equally full of darkness, viruses, click bait and offensive material. Stay away from the dark areas of the web when surfing.

The 's' in 'https' on the URL stands for secure. If the website is employing SSL encryption, 'https' will appear, as will a padlock. Make sure a site is secure before entering any personal information.

Read privacy policies. They provide information on what data is being collected and what is protected, as well as how that site tracks your online activity.

Use an ad blocker or pop-up blocker extension. This prevents any unwanted ads which contain spam or potentially harmful links to sites from appearing when you are innocently surfing the web.

Using WhatsApp

WhatsApp messages are encrypted, which does provide a high level of security to the user; however, it is absent mindedness that can cause the security of messages to be compromised.

Since the introduction of WhatsApp for desktop, there have been circumstances that have led to hackers or strangers to gain access to a user's entire message stream.

This occurs when someone carelessly leaves his phone unattended. It takes just a moment to scan his WhatsApp QR code and later implement this on a private PC to gain access to messages. This can be kept open indefinitely so they can continually monitor every message you are sending. It is recommended to enable the WhatsApp two-step verification feature to secure additional protection.

Using social media

Be careful not to overshare. Keep track of what you're posting. Your online persona can come back to bite you if not approached in the right way.

By posting about your daily activities on social media, you're practically inviting stalkers to extract your data and use it to make a profit.

Social media channels have a feature that includes location when posting. Disable this to keep your whereabouts private. This safeguards your personal security and belongings by preventing unwanted individuals from knowing where you are and when you are not at home.

Along with taking these preventive measures, it is also important for users to abide by the laws in the country related to the use of social media.

Sending/receiving emails

Don't click on any suspicious looking links, from trusted or untrusted sources.

If you get too many spam emails, spend some time unsubscribing from all of the email marketing you receive. This prevents the risk of clicking on harmful links too.

As you can easily see, protecting yourself, your data and your computer, takes just a few simple steps to ensure. By taking even basic care, you can make the most of the amazing new horizons that the Internet opens up for everyone, and actually use it to discover new avenues of growth in your personal life, career, business, social life and much more, without compromising your safety and peace of mind.

New game assesses your skills for cybersecurity industry

A new online game has been created to assess players on whether they might be equipped with the necessary skills to enter into the cybersecurity industry. The online platform has launched in the UK with a view not only to make an assessment of gamers, but also to try to make the cybersecurity industry appear more appealing to people.

2017 has seen more advanced forms of cyberattacks crippling organisations across the world, including the NotPetya and WannaCry ransomware. In order to provide the necessary protection from these malicious and damaging attacks, more experts are needed with a very specific set of skills.

James Hadley is the CEO of Immersive Labs, the company that has created the online platform. He says there simply isn't enough people studying computer sciences to fill all the roles needed, insisting that companies must search elsewhere and that the industry as a whole could benefit from the involvement of people from different educational backgrounds than the traditionally accepted route.

"People from non-technical backgrounds may bring new perspectives to what is as much a people problem as a computer one," Hadley explained. "Students with a wider range of experience would inject fresh ideas. Anyone good at analysing a situation, troubleshooting and problem-solving – or simply with perseverance and curiosity – fits the bill."

The platform is aimed only at UK students at this time, offering a range of training courses for beginners and advanced levels. A leaderboard will feature the top scorers and companies can then find potential candidates with a high level of competence to apply for roles.

Source: www.newscientist.com

Cyberspace Security Experts Warn: Reaper Botnet Malware is the biggest threat on the Internet

Cyberspace security experts have recently warned users that Reaper Botnet, which is an upgraded version of the malicious software Mirai Botnet, could significantly disrupt the Internet. Reaper Botnet has grown over short period and has spread to computers and IoTs with access to the Internet. It aims to exploit the vulnerabilities of non-updated devices in order to control them and add them to the command and control platform; this means they can continue to grow, and be harnessed by hackers to perform various extortion activities whenever they wish, as Denial of Service Attack.

The Reaper Botnet is an unprecedented destructive force that can spread and infect IT systems and grow to an extent that could disrupt services and access to resources on the Internet. A wide network of hacked devices has been identified, including WiFi and Router devices, Smart Web cameras, and computers, which can send huge amounts of destructive data to servers through a powerful wave that can cause malfunctions, or even disrupt Internet networks.

These cyberattacks can be widespread and aggressive. In addition, larger networks are at greater risk, because it is very difficult to address the spread of Reaper Botnet on all fronts at the same time and repair the damage caused by it.

It is worth noting that an extensive electronic attack has occurred earlier, when Mirai Botnet, the malicious software caused major disruptions on the Internet in parts of the United States. Despite preventive measures taken by the institutions and companies against cyberattacks and running the latest versions of basic software that provide the required security updates to handle this malware, many individuals (up to 80%) do not install software that includes updates that provide protection of malicious and unwanted software on all their devices, which puts their devices and data at great risk.

To ensure online security and provide information and data protection for individuals and businesses, especially with the increase in cyberattacks and the increasing number of computer devices with Internet access, cyberspace experts recommend the installation of software updates. This assures that computers with Internet access, whether at home or at the office, are not exposed to any damages or disruptions that may be caused by Reaper Botnet.

Source: www.sott.net

New controls considered for Power Grid protection

US grid operators will be required to take measures in guarding against the risk of malware, which could be infected by electronic devices, if proposals from the nation's top energy regulator are put into place.

The target is to nullify the risk from cyber criminals that could adversely impact the grid, the Federal Energy Regulatory Commission said in a statement.

The regulator is set to ask the North American Electric Reliability Corporation for criteria of electronic access controls for grid systems, before finding ways to reduce the threat posed by malicious hackers.

At the start of 2017, the Energy Department said that the electricity system faces "imminent danger" from cyberattacks. The events of the year thus far have helped to reinforce that position. If successfully hacked, a compromised grid could result in widespread power failures, also undermining national defence systems and damaging the economy of the nation, it said.

Source: www.bloomberg.com

Equifax breach has repercussions for credit industry

As 145 million Americans face up to the fact that their personal information has been compromised due to a breach of credit-reporting agency Equifax, it is the credit-rating sector that now has come under the microscope. The repercussions for half the population of America is that their credit could be ruined, their financial accounts stolen from, and their identities stolen, but the repercussions for Equifax are, at least for the time being, likely to be negligible.

The hack could have been prevented by the credit rating agency, as a known software vulnerability was ignored rather than instantly fixed, allegedly pushed to the back of the priority queue, allowing for hackers to take the details of every user registered with the organisation. The disaster was finally revealed to customers almost six weeks after Equifax discovered it, prompting calls from their customers to fine them, or at the very least bring in a law to make certain that companies are held accountable if they are to blame for any future compromises. In response to the calls, Congressman Greg Walden said: "I don't think we can pass a law that fixes stupid."

There is no question that organisations such as Equifax will always have a future. Their customers are not the public; they are the banks, credit card and mortgage providers of the world. To opt out as an individual of the credit rating system would be discount one's self from the economic world. Many won't do that.

But reform is likely to be just around the corner, starting with a responsible and upgraded approach to cybersecurity. One proposal gaining traction is to require Equifax and others to take out super insurance policies to compensate the public if anything recurs, but the criminal charges concept is the one the industry fears the most, and the one most likely to be pushed through.

Source: www.chicagotribune.com

Security on Social Media

How to improve your privacy and security on Social Media

Ihab Moawad, Vice President of Trend Micro: "A few minutes is all you need to protect your social media accounts."

Social media is, for better or worse, an integral part of life for many people, and an effective channel for communication with family, friends, and colleagues. It can also provide the main link between companies and their clients and companies and their suppliers. It has affected our way of life and our way of work, enhancing communication levels, ideas and the ability to share news, and stay informed about important information that could forever be kept under the radar by those previously in control of information dissemination to the public.

However, despite the benefits that go hand in hand with being the most informed generation for centuries, and being able to instantly connect with friends and clients across the world, social networks are not without risk – particularly to your personal details and information. Adjusting your privacy and security settings on your social media channels will enable you to secure your personal data to a great extent, and selecting the best protection option for your account requires only a few minutes.

In researching the most effective ways to maximise social media cyber security capabilities, Esharat interviewed the Vice-President of Trend Micro in the Mediterranean, Middle East and Africa region, Ihab Moawad. He begins by saying: "Social networks offer flexible communication methods, promote news sharing, and provide us with ways to navigate news and public events. However, despite all these benefits, social network sites are not risk-free, as anyone can see whatever you do, or want to do, or even your whereabouts. There have been a lot of hacking stories of personal information and using it for purposes that violate privacy and law. I would like to talk about providing a degree of protection and security to secure your personal page on any social media channel.

"Protection and security should be your main concern, as it is very easy for hackers to extract your data and use it to make a profit," Moawad explains. "My tips to improve your privacy and security in your social media accounts are firstly to review and adjust the settings each time updates are made to your account, ensuring that it conforms to the latest version. Adjusting settings may take minutes of your time, and as the saying goes, prevention is better than the cure."

On Facebook security settings

"Adjusting privacy and security settings for your Facebook page can be a bit confusing, but it depends on the security levels you want to apply. If you know the level of security you are looking for, modifying settings will be a very simple step.

"Facebook has made access to these settings very easy by clicking the lock icon located in the top right corner. You will find three sections with several options for setting privacy in your account: Who can see my stuff, who can contact me, and who can look me up. Recently, Facebook has created a simpler yet more comprehensive privacy settings page, which is worth reviewing," Moawad explains.

> Protection and security should be your main concern, as it is very easy for hackers to extract your data and use it to make a profit

"You can also improve your account protection by clicking Security in the Settings menu. Options allow you to adjust notifications, approvals, and application passwords as well as other account-related activities. The vast majority of users depend on the default settings, so you should review your security options to ensure that the account is secure against any hacking attempts, or to be able to have access to recover the account in case of loss."

Adjusting privacy on Twitter

"Due to the nature of Twitter, which is based on sharing ideas, the channel does not have a complicated level of privacy compared to Facebook, and so it is exposed to more hacking and data leaks. The two most important things to be secured in your Twitter account are your login verification and password reset. Do not confirm login verification requests. In order to make it difficult for anyone trying to gain illegal access into your account, you have to choose the 'Receive Login Verification Request' option," Moawad tells us.

"When it comes to a password reset, Twitter only requires a username. Therefore, you should raise your password security level by choosing 'Request Personal Information' (two-step verification) before resetting your e-mail notifications and text messages to ensure that your personal information will not be shared on any page or one of the public social media accounts."

"Likewise, with other social networks, post privacy settings will be disabled by default, which means that anyone, even if not a follower, can see your tweets. If you have an active account on Twitter and do not post personal information, then your account will be available to be seen by everyone. It is not necessary to protect your tweets, because this will make your tweets limited to your followers, and will not allow others to retweet them. Users will then have to send a follower approval request, and the replies you make to users who do not follow you (such as celebrities) will not be available to those users."

LinkedIn

LinkedIn is a social network dedicated to professionals around the world. LinkedIn allows you to connect with new colleagues, watch work-related videos, or share professional achievements. It allows job seekers to explore new job opportunities, or to communicate with former coworkers. Because it includes your CV, LinkedIn allows professional talent hunters to contact you and learn about your skills.

Moawad tells us: "Like any other social network, LinkedIn includes Security and Privacy Settings. Managing Your Account and Privacy Settings enables you to review and choose how to adjust posting activities, determine the possibility of seeing the page ranking, and choose what others can see on your personal page. It is a must to reset your password periodically to avoid hacking or piracy attempts.

Other social networks such as Pinterest, Foursquare, and Google Plus have useful setting tools to help you secure the privacy and security of your account. Finally, do not forget that securing your account doesn't only protect you; it protects your family and friends too."

The worst cyber-security breaches of 2017

2017 has been the year in which public knowledge of the severity of the threats one can be exposed to online reached an all-time high. This is largely due to the sheer volume of heavy-duty and high impact attacks that have rendered some of the largest multinationals, and millions of individuals, at the mercy of unscrupulous gangs of cybercriminals. Here, we take a look at the worst of 2017.

WannaCry

A strain of ransomware called WannaCry spread around the world, taking out public utilities and large corporations. It crippled the National Health Service hospitals and facilities in the United Kingdom. Microsoft had released a patch for the bug two months before the first wave of attack, but a number of organisations hadn't updated their systems. They then became infected.

Petya

Following on from WannaCry, Petya was a worldwide attack that took down some major corporations, but it was mostly targeted at disrupting the Ukraine, which it did. Infrastructure such as power companies, airports, public transit, and the central bank, were all badly affected.

Nearly 200 million US voter records released

A database was discovered, accessible to the public that contained the personal information of what some say is every American voter of the last decade. While not a hack, it was what's known as a misconfiguration that led to the security breach. This is a common risk to cybersecurity that can have savage consequences, however according to those that were responsible, nobody in the public domain found the records.

Equifax

Equifax is one of the largest credit agencies in the US, and suffered a serious breach that, it has been said, affects some 145 million consumers. The sensitive data that was stolen, and the sheer volume of it, made this one of the worst breaches ever seen. Names, addresses, DOBs, Social Security numbers, credit card numbers and other personal information were all compromised.

Ransomware
Viruses attack thousands of victims worldwide

The UAE is the eighth most targeted country for ransomware globally and the first regionally, according to Volume 21 of the Internet Security Threat Report by Symantec International Company, which specialises in Information Security Solutions. The growing number of phishing attacks against companies in the UAE can be attributed to the fact that the country is a central gateway to the Middle East region, with a world-class ICT infrastructure and an attractive business environment for investments, making it a trading hub for many international companies.

Dubai is working on enhancing its readiness to face the dangers of cyberspace security and protect the city's vital infrastructure against growing cyber threats. His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, launched in 2017 the Dubai Cyber Security Strategy that aims to strengthen Dubai's position as a world leader in innovation, safety and security. His Highness called for uniting the efforts of the government and private sector to ensure a secure cyberspace that makes Dubai digitally the safest city in the world.

The risk of Internet hackers using ransomware to blackmail companies is increasing. That risk is increasingly disrupting the electronic networks of major companies around the world. To put that in context, in 2017, the world saw the biggest wave of hacking attacks with ransomware. Those attacks affected more than 150 countries around the world and locked up at least 200,000 machines, most of which belonged to large companies and corporations, according to local and international media.

The ransomware virus still causes considerable disruptions and losses to electronic networks all over the world. Symantec Company, which specialises in the sale of software, especially in the field of information security and management, has identified more than 100 types of malware, which are increasing at an alarming rate and exposing companies and individuals to serious threats.

Ransomware is a relatively new virus in the realm of cyberattacks. It depends on the usage of a sophisticated malware that allows the hackers to access the operating system. It encrypts all data stored on a computer. It blackmails its victims, forcing them to pay money to unblock the operating system.

Should the victim refuse to comply with its demands, the virus deletes the files on the user's computer or keeps them encrypted indefinitely.

Ransomware usually uses an old method which involves sending a link or an email from an anonymous sender. Although the method is old, it is still tricky for web surfers, and it generates the best results for hackers. If the email draws the attention of the victim, and the victim decides to open the link and load it, he or she will fall victim the malicious intents of the hacker. In the year 2017 we have seen a significant rise in malware based attacks causing unprecedented disruptions around the world and infected hundreds of thousands of machines. The ransomware managed to encrypt the files of the target users and forced them to pay a ransom ranging between $300 and $600 per machine. The hackers demanded ransom payment within three days. If the user didn't pay, the amount of the ransom was doubled. If the ransom was not paid after seven days, the files were deleted.

It is worth noting that the first ransomware attack was initiated in 1989 by Joseph Popp, an academic from Harvard University, who participated in a World Health organisation conference on AIDS. In preparation for the conference, he prepared 20,000 floppy disks that contained "Information about AIDS" to delegates.

But what the delegates didn't realise was that the floppy disks contained a computer virus intentionally uploaded by Joseph Popp. After running the contents of the disks, the virus remained dormant on the victim's computer for some time. After the users restarted the computers for 90 times, the virus started to encrypt all the files on the computer and hide evidence. A message was sent to inform the users that their software would be restored after sending $189 to a mailbox in Panama.

It took another 16 years before anyone could implement Dr Popp's ransomware idea and use it as the Internet era was flourishing. However, the "zero-year," or the year when ransomware attacks started, was 2005. The "GP Coder" Trojan "infected the windows systems and files, and since then the ransom attacks continued to pose a growing threat on the entire cyberspace."

Esharat Magazine recommends that its readers avoid falling into the trap of ransomware by making sure they back up their devices' data constantly and avoid opening unknown links and downloading any files received from anonymous users through the email. It is also recommended that they use original and updated antivirus software and update their software constantly. They should also avoid access to suspected sites and assure they download programs and applications from its official sources. If you are infected by ransomware, you should not comply with the hackers' demands, stop all operations on your device or network directly and restore your backup.

5 Warning signs... Your computer has a virus!

There are so many different types of malware targeted at exposing vulnerable systems and gaining access to personal data, it's inherently important that we as individuals are able to recognise immediately if our computer system has fallen victim to an attack. Once we know we have a virus on our system, we are then in a position to look for a solution. Here are the five main symptoms of a malware infection or virus:

1. System crashes

If you find that individual programs crash, or the system itself crashes with any kind of regularity, there's a strong chance of infection.

2. Strange hard drive activity

If you notice your hard drive has been going on and off several times when you are not actually using it, it is advisable to check for malware and run a virus scan or even an anti-virus clean-up.

3. Pop-ups

If you find your computer screen being overcrowded by pop-ups despite you have not clicked on a link deliberately, your system might have a virus in it. An anti-virus scan is advised.

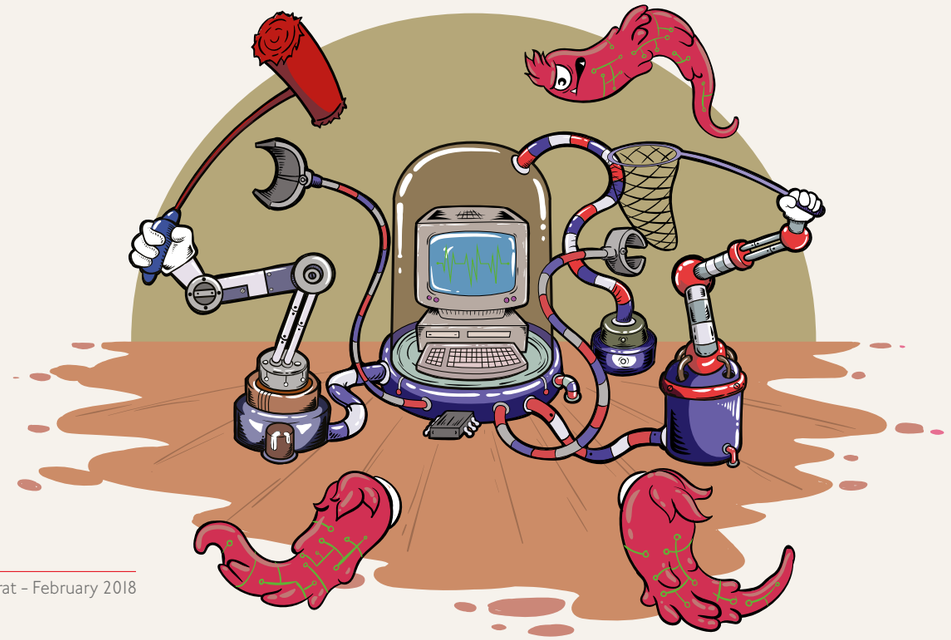
4. System slowdown

Malware will often slow down your system. If the system start up or program launches are taking noticeably longer, it either means your system memory is lacking, or you have a virus.

5. No space

If, out of nowhere, your hard drive is full, or a notification often flashes up warning that disk space is getting low, there's a good chance your system may have become infected. Malware can often fill up a hard drive very quickly.

*If you suspect your system has been compromised or infected, we provide the steps you should take to secure and eradicate any viruses on the next page.



What to do if you've got a virus

If you've clicked on something you really shouldn't have and your computer is now infected with a virus or malware, it's important to take quick action to stop your files from being lost and to prevent your computer and online accounts being used to attack others.

These are the steps you need to take to try and get back to normal as soon as possible after being the victim of a hack.

Go offline

First thing's first. Cut off the WiFi connection you're using for the computer. No network, no point, at least from a hacker's point of view. If they can't communicate with your computer, it's of no use to them.

Shutdown and remove the hard drive

Immediately, as soon as you're sure you have a virus you need to shut down your system. Once shut down, remove the hard drive, connect it to a secondary computer (with a full suite of anti-virus software installed) using a hard drive caddy connected via USB.

Perform a scan

Using the anti-virus software installed on the second system you've connected to, perform a full scan to detect and remove the infection from the hard drive.

Backup

Backup everything on the hard drive of any value or importance. Save the content on to a CD, another hard drive or cloud storage.

Put your hard drive back

If your files are backed up, you may seek the help of an IT expert to put your hard drive back in your original PC and begin the recovery process.

Wipe your hard drive

Despite the fact that the anti-virus scan shows the threat to have gone, it's not a guarantee and the only way to ensure this is to completely wipe the drive and then download your operating system again, from a trusted source of course.

Install updates

Make sure to download all updates and patches for your operating system before you install anything else.

Install anti-virus, anti-spyware, and other security software first

Before you use the computer, you must install as many layers of security as you can. You must also ensure the latest patches and updates are there. Failure to do so could result in damage coming once again.

Scan your old files for viruses before installing them

It now seems like your system is in the clear, and you can re-upload all of your files. However, you should always scan all of those files you downloaded to a disk or uploaded to the cloud before.

Backup your system

You should do a complete backup of all your files so if a virus ever finds its way onto your computer again, you won't need to go through this entire process once more. Backups should be done once a month minimum.

Create a Strong Password

How to create a killer password that can't be hacked

Passwords are an essential component of modern Internet use through laptops, smartphones and tablet devices. Protecting your privacy by using strong passwords is now an indispensable requirement as Internet use increases. Financial and personal information, health data, and private documents, as well as emails and photos are now stored and accessible online, and if hackers can get their hands on this information, they will more than likely use it against you.

Every day, thousands of users get hacked across the world, resulting in severe moral and material loss. The research unit at Wells Fargo Bank estimates that hackers cost companies $180 billion annually, while inflicting direct material damage of $12 billion to individual consumers, in addition to the time needed to recover the stolen data.

But how can you create an unbreakable password? To answer this question, we must first identify the common password mistakes people make, and learn how hackers work.

What is a hacker?

Some people assume a hacker is someone who attempts to hack accounts, trying to figure out passwords, having a few tries and then moving on to the next one. But that's totally wrong.

Hackers use sophisticated software that attacks the target account relentlessly and is able to try out up to 1,000 possible combinations per minute. That way, the combination of your account password is cracked.

What is the common mistake you need to avoid when creating a password?

An Internet-related study shows that one in ten people use the password 1234, and tens of thousands use common passwords that are far too easy to predict because they are based on personal data, such as birthdays, phone numbers, mail addresses and their kid's names.

A study conducted by Lancaster University reveals that "the main reason behind using easy passwords is that people are unaware of the risks." Dr Jeff Yan, co-author of a paper on password cracking says: "A main reason I think is that they're either unaware of or don't understand the risks of online security."

How are passwords cracked?

Passwords are cracked using various methods, such as using special software that attempts to access the target account by firing off thousands of password guesses per minute. If this method doesn't work, the hacker will resort to a brute force attack by gaining access to company data and acquiring a database of millions of passwords to decrypt and use. If decoding encrypted passwords fails, the hacker uses hacking software to guess and crack the password of the target account. He or she usually succeeds - if the password is easy.

For this reason, experts advise you to choose strong, complex and hard-to-guess passwords that are made up of different letters, numbers and symbols. You should also change it approximately every ten weeks.

Extra security from two-factor authentication

Now, you are usually given the option to get two-factor authentication, whereby a code is sent to your registered mobile number or email address which is valid for a limited time. It is recommended that in addition to creating a complex password, you also make use of the two-factor authentication method.

Source: *www.theguardian.com*
securingtomorrow.mcafee.com

Tips for creating a secure password

For almost every account that you create online, you are required to enter a very secure password that's difficult for hackers to guess when they first attempt to hack any of your accounts. You will find below some important tips on how to create a strong, secure and hard-to-figure out password.

- Avoid commonly used passwords, even if it's an Arabic password written in Latin letters.
- Choose a password that contains at least 10 characters, and always mix letters, numbers and symbols. It is also recommended to use the maximum number of characters permitted by websites.
- Avoid using your favourite sports in your password, such as f00tbAll or basketball777 etc. Do not also include any personal information in your passwords and do not share this information on social media sites, such as Facebook, Twitter or Instagram. Hackers can easily gain access to these accounts and use your information to figure out your password.
- Do not store your passwords on your computer or phone.
- Avoid repeating letters, numbers and symbols in your password.
- You should never use the same password on multiple accounts. If you do this, and a hacker is able to figure out your password for one account, he or she will be able to access all of your accounts.
- Change your passwords regularly. For online financial accounts, it's probably a good idea to change them every month, and every three months for other accounts.

How to find out if your WordPress site has been hacked

One of the favoured approaches for cybercriminals to get their malware out there is to launch attacks targeted at websites. There are a few reasons for this. Firstly, website owners tend to adopt a rather blasé approach to the security of their site – certainly it's less of a concern to many than their own social media accounts. Also, if the website gains a lot of traffic, that's a lot of potential users they can target. A website that has gained the trust of its visitors means they will often think nothing of clicking on a link within it, regardless of whether it appears to seasoned experts as somewhat suspicious.

Anything that is open source, will have probably at some point been targeted by hackers, and although WordPress leads the way when it comes to security, it is far from infallible. The fallout resulting from a WordPress hack for the site owner can be very damaging, leading to mistrust in users, reduction in traffic, and sometimes even a complete loss of archived material.

Here are some of the signs that your WordPress has been hacked:

Emails start to bounce

Usually this will happen because hackers use your account to send thousands of spam emails from your IP address. These are then marked as spam by numerous recipients, and thus your email address very quickly gets blocked.

Content you didn't publish gets published

If your site has been hacked, the hackers will find it quite easy to add and publish content. The results can be devastating, and can range from bad links to completely different content that you wouldn't want to be associated with.

Website is slow

This could either be a result of the hacker adding such a great deal of code into your site, or you may have been added to a network where traffic is auto-directed to your site in order to get to a target site or page.

Traffic disappears

If you've been the victim of a hacking, Google will be among the first to know, and they will let their users know. You'll be blacklisted and a warning will appear next to your listing if anyone even finds you. If your traffic has gone down significantly, you may have been hacked.

Traffic increases

A lot of WordPress sites receive traffic from countries that owners would not expect many visitors to come from. These are usually bots utilised for many purposes such as site mapping and ranking by search engines and in some instance bots can be configured with bad intentions by trying to find a weakness. If the traffic increases from other countries that stand out as not really being among your target audience, there's a chance a weakness has been found.

Your website disappears

When a site is hacked, your website may no longer be accessible. Often your host will take it down to protect web users, and the corrupted files must be managed and removed manually – usually by you, although you can pay the hosts or one of their partners to do it for you.

As a website owner or manager, it is important to constantly monitor the site, keep it updated and backed up on a monthly basis. You should also enable auto-updates on your server to ensure your website has the latest security patch. These are the best ways to defend a hack, and this approach to website management also places you in a strong position to withstand the numerous attempts at a hack your website may be subjected to each day. If it is compromised, you can react and take measures quickly and efficiently by constantly monitoring activity on your site and identifying anomalies.

Protect Your Organisation

How to protect your organisation from cyberattacks!

It begins with ensuring you adopt the latest international security standards

A report published by Deloitte states that the wealthier the nation, the more susceptible it is to a targeted cyberattack. The biggest targets are the UK, the USA, South Korea and Japan, according to the report. Certainly the image the nation portrays is one that is likely to immediately catch the attention of cyber criminals.

Cybercrime already costs businesses $400 billion worldwide annually according to a study issued by the Center of Strategic and International Studies.

Cyberattacks are damaging to businesses in more ways than just the immediate theft of money. There is the threat of reputational damage, trade difficulties and overall growth impediment.
In developed nations the effect of cyberattacks on businesses has serious implications for employment rates, and although you may feel your organisation is safe from an attack or is not a target, you've just made your first mistake.

It is critically important now to safeguard your information and data. Your systems and networks should be treated like the front door of your house. Perhaps in the fifties or sixties you could get away with leaving your door unlocked, but now we live in a very different world.

Internal policy

The biggest cybersecurity risk for an organisation is its employees. There are countless examples of criminals gaining access to systems and networks because of an employee's actions. This could be clicking on a bad link, using a weak password (123456 is not a password, it's an invitation), and in some other cases it has been disclosure of information over the telephone to somebody with an assumed identity.

Scams are everywhere and they are also continually evolving. Staff awareness is something to be taken very seriously indeed.

Update your software and apps

Whenever a notification about an update is received - and this could be from your Operating System or your security software, it's important that this is actioned immediately or else it is open to the more advanced attacks it has been updated to negate.

Speak to an expert

Most of us know only the very basics of Internet security. We can change our passwords regularly (although most of us don't) and we can come up with increasingly complex combinations of numbers, letters and characters (although most of us don't); we can even download the latest firewall software. But there is no substitute for hiring an expert to advise, assess and test the systems. Cyber criminals will quickly locate the area of vulnerability, so it's important to get an expert to do so on your behalf before them and get it fixed.

This may sound like an expensive option, but in reality there must be a vision in place that comprehends the depth of the damage further along down the line if an attack compromises the data of your organisations. One needs only to ask Yahoo, IBM, Lloyds, Sony, Facebook, Twitter and even Apple. These huge companies will help clarify the damage they each sustained when targeted by cyberattacks.

Krack reveals the need to update or remain at risk from using WiFi

Hackers can now target anyone using WiFi, according to a startling revelation revealed by a Belgian researcher from the KU Leuven University.

The researcher, named Mathy Vanhoef, has released information on his own hack, dubbed 'KRACK' (Key Reinstallation Attack), and what it purports is quite astonishing. This hack allows hackers to decrypt and look at everything everyone is doing online if they are on a WiFi connection. Not a public WiFi connection – any WiFi connection.

This bug, which Vanhoef announced on his KRACK website, comes with the following claims: "This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected WiFi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites."

The vulnerability here comes with the WPA2 encryption protocol – something we have all at some point used or are familiar with. This is used by most WiFi users to keep their session private. KRACK works by effectively fooling the user into re-installing an encryption that is already in use.

Normally, an encryption key, which represents an agreement between the WiFi router and the device/computer with which it's connected, are unique and are for one use only. As the agreement is struck and the connection is made, encryption keys are generated and a one-time number is created. Now, it has been revealed that an attacker can manipulate this initial meeting through WPA2 so as the apparently new and unique key can actually be one that is old and in use. This enables the hacker to silently intercept all data coming and going through the network.

It is Android users who are most at risk, it's claimed, as a coding error has been identified that enables the hacker to find the key by forcing a reinstallation. The operating system uses an "all-zero encryption key" which is easier to intercept for malicious purposes.

The bigger picture is that any device which uses WiFi is at risk. As Vanhoef explains, "The weaknesses are in the WiFi standard itself, and not in individual products or implementations. Therefore, any correct implementation of WPA2 is likely affected. To prevent the attack, users must update affected products as soon as security updates become available. Note that if your device supports WiFi, it is most likely affected. During our initial research, we discovered ourselves that Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys, and others are all affected by some variant of the attacks."

This means that if WiFi users haven't already, they must update all their devices and systems that use WiFi with immediate effect. This includes computers, smart devices, tablets, games consoles, TVs, radios and car systems. Failure to do this could have serious consequences for the user, including the loss of all personal information such as passwords and bank details.

KRACK comes as a huge wake up call to the global electronic security, as private WiFi networks were previously thought to be one of the most trusted environments around. This fundamental flaw in the specified protocol has left billions of users open to being targeted although the route for a remote attack is complex and unlikely in truth due to the need to be within close proximity of the device itself. However, it has raised question marks over whether other flaws might be exposed in general settings that all users have been led to think safe. The white hats will be hopeful of uncovering these flaws before the black hats.

Source: www.forbes.com