ISSUE 01 JULY 2017

إشارات Esharat

Dedicated to a safer cyberspace

HH SHEIKH MOHAMMED BIN RASHID AL MAKTOUM ESTABLISHES DESC TO MAKE DUBAI THE SAFEST ELECTRONIC CITY IN THE WORLD

THE INVENTOR AHMED AL HAMMADI

10 TIPS FOR PROTECTING AGAINST CYBERCRIME

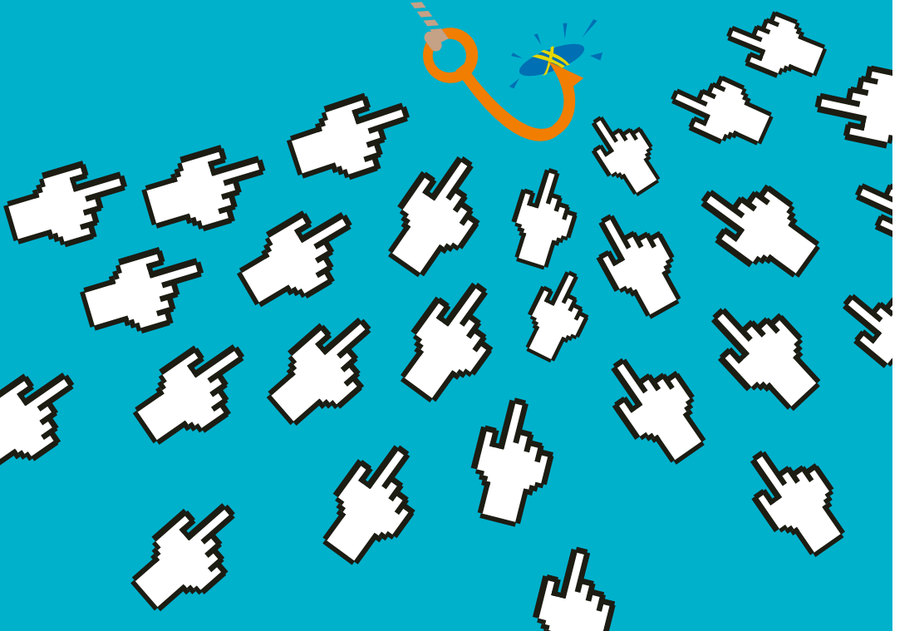
"WE WANT TO MAKE DUBAI THE SAFEST ELECTRONIC CITY IN THE WORLD" AMER SHARAF

KEVIN MITNICK: NOTHING IS UNHACKABLE

THINK BEFORE YOU CLICK

Hackers want your personal information, and they will try every trick in the book to get it. An infected computer or hacked email address puts your personal information and the information of others at risk! Always be certain that any link you click on is from a trusted source.

BE VIGILANT, STAY SAFE



مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

A magazine specialised in cyber security and technology, issued bi-annually and produced on behalf of the Dubai Electronic Security Center

General Supervisor:
Yousuf Hamad Al Shaibani

Managing Editor:
Amer Sharaf

Editorial Secretary:
Shaikha Essa

Editorial and Design:

7G MEDIA

Editorial Board:
Amani Abuseedo
Dan Charter
Ahmed Mersal

Design and Production:
Sree E S
Aws Rahhal

Illustrator:
Brian Reyes

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

INSIDE

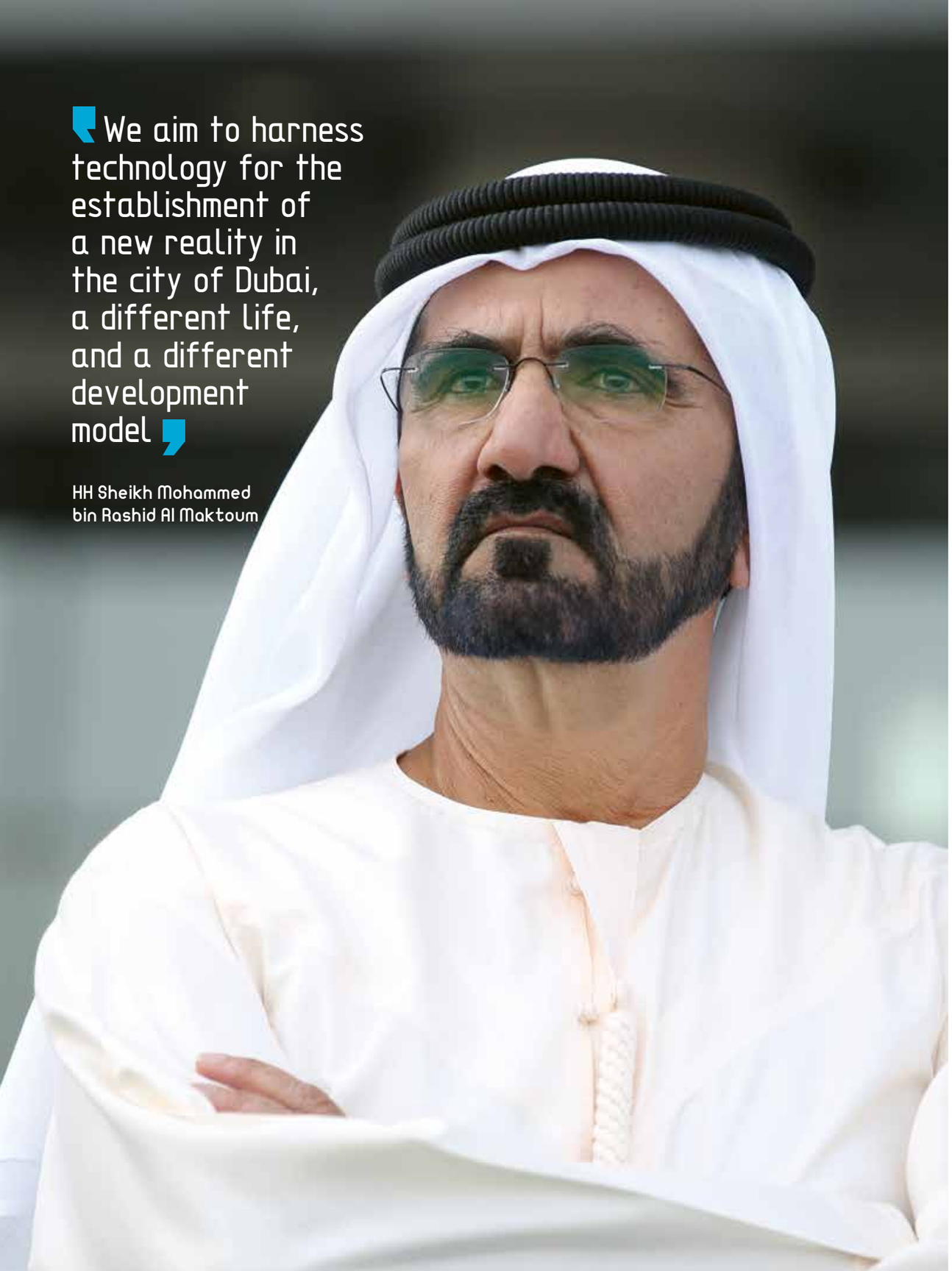
Creating a safe cyberspace

Over the past thirty years, the world has shrunk twice. The first time it turned into a small global village, as communication and technology experts used to say, before it then turned into a small electronic device that fits in the palm of your hand. The digital world is now closely related to our real world. By just using a smartphone, we can build strong ties and make online transactions. Now, any official document can be applied for using smart services. We can also make travel and hotel reservations, as well as purchase goods and services using our smart phones. Making payments online is now a matter of routine. Engaging in e-commerce, doing business and applying for services online have become realities in our new world. Furthermore, social networking sites have become our way to keep up with close social ties and they have clearly changed how we interact and communicate with others.

This transformation has made it incredibly easy to start new relationships and meet new people online. However, it presents new challenges. With smart cities, cloud computing and the Internet of Things, came online fraud, organised crime groups, spyware and impersonation. Although there is no physical interaction, these risks can spill into the outside world and present serious threats to our social lives, bank accounts, our personal security, as well as our families, children and our loved ones.

Creating a safe and reliable cyberspace is our only way to have a navigate this new world without trouble. While Dubai Electronic Security Center (DESC) builds a wall to protect our institutions, companies and city, the enormous challenges facing Dubai in its journey to be the smartest and most innovative city in the world require establishing cooperation ties between the public sector on one side and the private sector, universities and individuals on the other. This unification will form a reliable shield against online fraud and organised crime. Accordingly, we present to you Esharat Magazine, issued to raise awareness among individuals, companies and all those who do business online, use online communications and social media with the goal of creating a safe cyberspace where everyone knows their rights and obligations in terms of how to defend personal security and the security of the nation as well.

Yousuf Hamad Al Shaibani
Chief Executive Officer
Dubai Electronic Security Center



His Highness Sheikh Mohammed bin Rashid Al Maktoum establishes DESC to position Dubai as a global leader in innovation, safety and security

His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, established Dubai Electronic Security Center (DESC) in 2014, to make Dubai the safest electronic city in the world, and to develop and implement the emirates' information security practices and set good-practice criteria for cybersecurity.

HH Sheikh Mohammed bin Rashid's vision for Dubai was the inspiration for the Dubai Plan 2021, a plan that maps out the targets for the next five years in the emirate. Two of the core components of the plan are to make Dubai the most secure place to live, while also creating a smart, integrated and connected city. In this regard, DESC has a strategic plan to contribute towards the accomplishment of these two objectives, but also to deal with electronic security threats, cyber attacks and all forms of cybercrime.

The cybersecurity strategy issued by DESC targets comprehensive protection against all cybersecurity risks for Dubai, while also supporting innovation, growth and economic prosperity. The strategy covers a five-year period up until 2021.

DESC works alongside all entities within the Dubai government to ensure that their cybersecurity awareness, precautionary measures and systems are of an internationally comparable standard. In order to achieve the objectives set in place through the strategy, DESC relies on cooperation from all government entities, so as Dubai can be a leading secure cyberspace. The five objectives are as follows:

Cyber-smart society

DESC ensures there is the availability of knowledgeable personnel ready to train individuals and employees within the public and private sectors on cybersecurity, offering full support. A cyber-smart society positions Dubai in a strong position, as awareness of the latest cyber threats is the key to achieving the highest level of cybersecurity in the city.

Innovation

The centre works to promote research and development projects within the field of cybersecurity, all targeted at establishing a free and fair cyberspace in Dubai, with the highest level of security.

Cybersecurity

DESC is set to implement a set of controls that protect the privacy and integrity of individuals, public and private entities within Dubai. The centre will also implement and develop an Information Security Management System (ISMS) standard, and will work to ensure that all senior executive level management employees have an understanding the importance of cybersecurity.

Cyber resilience

The centre is the first port of call for any cyber threats or incidents among government entities, and is dedicated to ensuring that should an attack or disruption occur, business continuity is assured. DESC provides a platform for incident management and a platform for information sharing.

National and international collaboration

DESC will lead Dubai towards establishing new national and international partnerships with a view to collaborating so as to manage cyber threats and risks. DESC will also establish the cyber security regulation based upon leading international methodologies and experiences.

National collaboration is also one of the focuses of HH Sheikh Mohammed bin Rashid's vision, which recognises that the key to accomplishing a nation and city capable of competing with the leading destinations around the world relies ultimately upon the talent and working methodology of those working within government.

DESC targets comprehensive protection against all cybersecurity risks for Dubai, while supporting innovation, growth and economic prosperity

HH Sheikh Mohammed bin Rashid offcially launches Dubai Cyber Security Strategy

> Cyber security is essential as we connect to the world using new, smart technology

His Highness Sheikh 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, has launched the Dubai Cyber Security Strategy, targeted at strengthening Dubai's position as a world leader in innovation, safety and security.

The strategy was launched in the presence of His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai and Chairman of the Executive Council; His Highness Sheikh Ahmed bin Mohammed bin Rashid Al Maktoum, Chairman of the Mohammed bin Rashid Al Maktoum Knowledge Foundation; His Highness Sheikh Mansour bin Mohammed bin Rashid Al Maktoum and His Excellency Mohammed bin Abdullah Al Gergawi, Minister of Cabinet Affairs and The Future, alongside Deputy Chairman of Dubai Police Lt. General Dahi Khalfan Tamim and General Security of Dubai Police Major General Talal Humaid Belhoul.

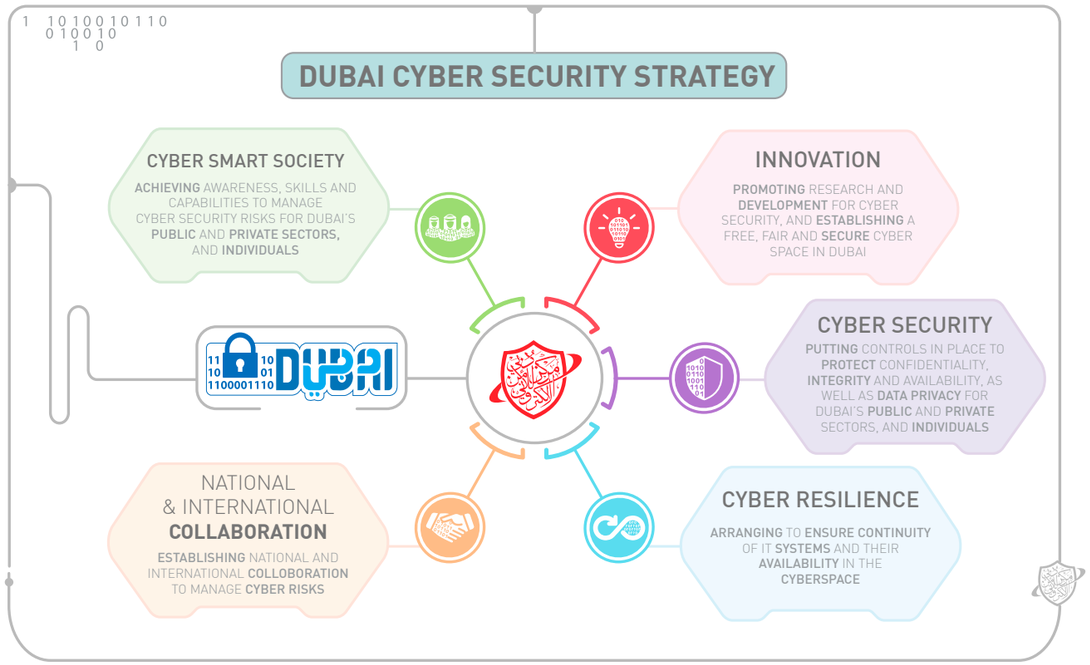
HH Sheikh Mohammed bin Rashid Al Maktoum highlighted the UAE's high global ranking in its provision of security for residents and organisations. His Highness said that this level of protection comes as a result of the efforts of federal and local governments in the UAE to build a safe and secure environment, which ensures the success of development goals.

His Highness also noted that cyber security is now an essential requirement as the world is connected and an influx of smart technology continues to be produced rapidly. HH Sheikh Mohammed stressed the importance of developing strategies to maximise the benefits of technology, while ensuring we are prepared to face any challenges technology may bring us.

HH Sheikh Mohammed said: "We have set ourselves firmly on a path of excellence and creativity in the UAE, and today with the launch of the Dubai Cyber Security Strategy we are adding a new achievement. This proves to the world that the more challenges we face, the more determined we are to achieve the highest level of excellence," before he urged both the government and private sectors to unite and ensure a secure cyberspace that makes Dubai the safest electronic city in the world.

The Dubai Cyber Security Strategy provides integrated protection against the dangers of cyberspace, support for innovation in cyberspace and the growth of Dubai and its economic prosperity.

Two core components of the Dubai Plan 2021 are to make Dubai the most secure place to live, while also creating a smart, integrated and connected city. In this regard, the strategic plan of the Dubai Electronic Security Center contributes to the accomplishment of these components while dealing with electronic security threats, cyberattacks and all forms of cybercrime.



The Dubai Cyber Security Strategy involves the implementation of five main domains under the following headings:

Cyber smart society: Raise public awareness on the importance of cyber security, the dangers of cybercrime, and the methods to minimise exposure to criminals.

Innovation: Igniting innovation and scientific research in the field of electronic security.

Cyber security: Build a secure cyberspace, protecting the confidentiality, credibility, availability and privacy of data.

Cyber resilience: Ensure continuity and availability of IT systems in the event of any cyberattacks.

National and international collaboration: Establish local and global partnerships to cooperate in confronting threats and risks in cyberspace.

"We want to make Dubai the safest electronic city in the world." -Amer Sharaf

Amer Sharaf is the Director of Compliance Support and Alliances for DESC. He studied his bachelors in Computer Science and Masters in Computer Information Systems at Boston University in the US, before returning to the UAE and working for Dubai Police in the IT department. His passion, as he says, is to "make sure that all government departments are aware of the need for vigilance towards the threat of cybersecurity."

Sharaf's team is working on the Information Security Regulation which will become a regulation for government departments by mandate, and his role is to achieve the DESC vision of making Dubai the safest electronic city in the world. Esharat spoke with him to find out, for those that may not have heard of DESC, exactly what they do, and to explain why cybersecurity is so important for the UAE.

Esharat: Tell us about the role of the center and its objectives.

Sharaf: "Dubai Electronic Security Center (DESC) was established in 2014 under the mandate of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai. The vision of DESC is to make Dubai among the safest electronic cities in the world. Our function is to protect information, which relates to the electronic storing and sharing of data and material between government departments. There are many functions that fall under that particular aim. Another aim is to develop the necessary means to provide a high level of electronic security. We develop existing tools and solutions to further enhance our security. Security Incident Event Management (SIEM) tools are a good example of this; we utilise SIEM tools to measure traffic to see if there's any ambiguous anomalies to detect if any potential attacks are happening."

Esharat: How does DESC protect the government networks?

Sharaf: "There are several ways in which we protect the government networks. One of these is to help the government networks establish the much-needed security operations center from which they will be able to have oversight on their network's activity and track unusual traffic and behaviour. Additionally, DESC provides advisories to all government departments sharing with them information on how to protect themselves from recently found vulnerabilities. From a proactive perspective, DESC provides cybersecurity awareness training to key people in each government department, who in turn will

> DESC aims to develop the necessary means to provide a high level of electronic security

> Our policy is called the Information Security Regulation, and this applies to every government entity by mandate

be responsible to train the employees within their respective departments."

Esharat: What action do you take when a threat is identified?

Sharaf: "Should we or the government department notice any unusual activity, the action that should be taken is to first isolate the issue and control any possible information breach that may be occurring, taking the necessary countermeasures. After isolation, you should then study the root cause and ensure that the same doesn't happen elsewhere. It's important that incidents are reported to the management and to DESC. We will then assess the nature of the vulnerability or attack faced in the incident and share only the lessons learned with the rest of the departments so that they can protect themselves from it. Although we all know that absolute security will never exist in the cyber space, we should always work to detect any ambiguous activities in our networks and stop them before they expand. There are many technologies available today that always help us to have a live monitor of suspicious activity and to quickly take the necessary actions to block the threats."

Esharat: What sort of information would a hacker try to access from a government entity?

Sharaf: "Sensitive and personal information that is private should be classified accordingly and protected from unauthorised access. For government networks, hackers could be targeting employee lists, addresses, emails, passwords, national ID numbers for example, and this information could leave individuals susceptible to identity theft or any number of serious crimes. In many cases hackers try to impact the reputation of their targets. This is usually done by exposing personal information or defacing websites causing financial loss. Hackers may have more destructive intentions, and so could be looking to disrupt services of their targets by wiping clean their target as seen with the recent Shamoon cyber attacks in Saudi."

Esharat: What is your own role at DESC?

Sharaf: "It's a two-part role. The department I manage has two main responsibilities; the first part is compliance, where we work with government entities to help them adhere to the information security policies and regulations issued from DESC. Let's start with the policy we have today: Our policy is called the Information Security Regulation, or ISR, and this particular regulation applies to every government entity by mandate and was implemented in 2012. We enhance, update and develop this regulation to make sure it's updated with the latest developments in the cybersecurity field. We then distribute it to the government departments to adopt.

"Also we are able to create new policies that oversee and maintain the integrity of information security. These policies are then distributed to all government departments and we have a team that actually does the audit, ensuring they are all compliant with the latest regulations. The essence of this is to ensure information security at the heart of the government. We visit each and every department to clarify that each of the 388 controls within the regulation are being met up to the expected standard."

Esharat: Are you visiting a different department each day to conduct an audit?

Sharaf: "At our current capacity we are conducting 1-2 audits per week depending on the size of the entity being visited. As the audit team resources expand so will the number of government departments we can cover per week. To date there are over 140 government departments in Dubai obviously with varying sizes in terms of number of employees and locations. The audit covers the entire 12 domains of the Information Security Regulation (ISR) which has 388 controls. The ISR is an Information Security Management System which helps to provide Dubai Government Entities with the standards to ensure business continuity, and minimise information security related risks and damages by preventing or minimising information security incidents."

Esharat: And the alliance aspect to your role?

Sharaf: "The alliance part of my role is related to collaboration. DESC needs to collaborate in many ways; with similarly minded national and international entities to form bonds and relationships through which we are able to share knowledge about general and targeted cyber threats. Only together can we truly fight these threats.

"The alliance aspect of my role also covers PR and media where we plan and communicate our messages through the various channels that we have established."

Esharat: To make Dubai the safest electronic city in the world, that's a big job. How far are you towards accomplishing that vision?

Sharaf: "To be the safest electronic city in the world is an endless journey, as we have to continuously strive and keep ahead of the threats and challenges facing the city. That's why you need to adapt and learn from all the new trends that are appearing all around you. From that you will always be able to enhance and improve. It's a cycle. It never stops."

Esharat: What is your evaluation of the level of security and awareness here in Dubai?

Sharaf: "That's a very good question and I can actually align it with some of the initiatives we are doing here. For us to reach an adequate and acceptable level of information security, certain things need to happen. The Information Security Regulation is just one of these; awareness is another. We have a cybersecurity strategy which we are planning to launch very soon. It's actually completed and we have held several workshops on that with our strategic partners (government

"The vision of DESC is to make Dubai the safest electronic city in the world"

departments). It is part of our mandate to come forward with a strategy for Dubai. The strategy has its own vision, which is to establish Dubai as the global leader in innovation, safety and security. This will be achieved through five domains which cover all the important aspects of electronic security that have been benchmarked internationally to make sure we conduct our activities at a comparable international standard. Cybersecurity; a cyber-smart society, which relates to awareness among UAE nationals and residents; cyber resilience, ensuring availability of systems and solutions and business continuity; innovation, to innovate in the field of cybersecurity, promote research and connect with research centers in universities; and the final one is collaboration nationally and internationally. It's an exciting strategy that will really boost Dubai's security by 2021."

Esharat: Isn't the main threat to the security of Dubai government entities the employees themselves? As so many of the high profile data breaches have been caused by an employee clicking on a bad link, or as you mentioned with the Shamoon attack. How do we counter that threat?

Sharaf: "You're right, and in the end it all comes down to the awareness of the individual. The regulation that we've put in place requires awareness to happen. It simply must happen - for the employee, and for individuals. Through the strategy we are trying to reach everyone in society, not just government entities. Our scope relates to the government of Dubai, so we reach out to the departments responsible for a particular segment of individuals. With awareness, each authority can assist us with putting forward the vision of the strategy to make sure awareness reaches everyone in Dubai. Awareness is key, and it's not just a one-time thing. It's a repetitive cycle that has to happen periodically. Part of our auditing process is to make sure this is happening and that evaluations are carried out. We ask to see the results to make sure they are adopting this approach. It's crucial to what we do."

Esharat: What are the reasons for attacks generally? We've have seen many politically charged attacks recently, or so we are led to believe. Is that something that happens?

Sharaf: "The potential for attacks targeted at political gain is there, as is evident today on a global level. It's all related to the time and the events that are happening. But what›s popular nowadays is the use of ransomware for financial gain rather than political. This is a trend that is really growing. If you become a victim of ransomware your data is encrypted rendering it inaccessible and you must pay a ransom to have it decrypted. I think ransomware is a prime example of how the criminal landscape has changed, where in the past it used to be a physical act."

Esharat: How can everyone be more secure?

Sharaf: "It's very simple actually, just by looking at the statistics and learning from what history has taught us so far, it's all about the individual. If the person is given attention and awareness in the right way with the right level of dedication, then things would change a lot. Establishing procedures and policies, and acquiring sophisticated software and systems are all important, but the key is to focus on the individuals."

Hackers can get security pin from how users hold smart phones

Hackers can steal mobile device users' pin numbers from the way their phone tilts when they type on them, a new study has shown.

Researchers at Newcastle University in England were able to guess a four-digit pin with an accuracy of 70% using the data from gyroscopes installed on every modern smart phone. By the fifth attempt, the computer scientists achieved 100% accuracy.

This hack targets an anomaly in the way that web browsers share information. Sensitive information, such as current location, requires permission, however information which is widely regarded to be non-sensitive and of very little consequence is shared without acknowledgement. A malicious website therefore is able to ask for and obtain device orientation quite simply.

To program a system capable of identifying pins from phone angles is not a simple procedure, however, and the researchers required a great deal of data from users before they were able to guess their pins. This included the submittal of 50 known pins they have or would consider using.

It does however flag up a concern about exactly who is accessing what data derived from users' smartphones. By allowing a website access to locations, and even cameras, users effectively have no control over how that permission is effectuated. This can be hugely risky for the user in a world where hackers are resorting to more underhanded and complex trickery in order to gain what they want.

Dr Maryam Mehrnezhad, a research fellow in the School of Computing Science, said: "Most smartphones, tablets, and other wearables are now equipped with a multitude of sensors. Because mobile apps and websites don't need to ask permission to access most of them, malicious programs can covertly 'listen in' on your sensor data and use it to discover a wide range of sensitive information about you, such as phone call timing, physical activities and even your touch actions, pins and passwords."

In research from 2014, hackers were able to extract pin codes using the front camera of a smart phone by studying the eye of the user as they typed their pin.

DESC offers employment opportunities at Careers UAE 2017

Dubai Electronic Security Center (DESC) participated for the second consecutive year in the Careers UAE fair, held at the Dubai World Trade Center between the 9th and 11th April 2017.

DESC's participation comes as a reflection of the emphasis it places on attracting promising, qualified Emirati talents who are capable of contributing to the accomplishment of the continuously updated plan for DESC. The center will also provide opportunities for career advancement in various disciplines, and will offer job seekers a wide range of career opportunities, including technical and administrative job openings.

The center provides a working environment that embraces innovation and creativity, which is in line with the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, to forecast the nation's future and accelerate the pace of development so as to cope with technological advances and innovation across the world. The center aims to achieve its goals and objectives through innovating state-of-the art technology and solutions applied to information security, the communication networks and information systems of the Government of Dubai.

Believing that building nations can only be done from within, DESC follows sound and clear plans to build human capacities according to the directives of His Highness Sheikh Mohammed bin Rashid Al Maktoum, who said: "Building human beings is the key and building nations is not complete without building citizens, who are the real wealth."

DESC attends ACM Conference on Computer and Communications Security

Dubai Electronic Security Center (DESC) participated in the ACM Conference on Computer and Communications Security hosted by the New York University at Abu Dhabi in cooperation with the center, for the first time in the Middle East. The conference is one of the region's most important cybersecurity events covering a wide number of technical topics around recent cybersecurity-related threats and challenges.

The conference topics shed light on the importance of building collaborative research relations between the government, industry and academia in the UAE to stimulate a dynamic environment in the development and construction of innovative security solutions in the UAE.

Dr Marwan Alzarooni, Director of the Information Services Department at DESC delivered a speech that stressed on the center's main objectives, which are to protect all Dubai government and semi-government department information, communication networks and information systems, as well as enhancing, adjusting and implementing the necessary methods in the realm of cybersecurity and raising efficiency of information storage and exchange.

His Excellency Yousuf Al Shaibani, CEO of DESC, endorsed the important role that local research and conferences play in transferring and building knowledge in the UAE in the field of cybersecurity and ultimately amongst researchers, experts and attendees. He also added that: "DESC closely collaborates with universities and research centers to support information security research projects and empower students with the necessary tools and knowledge in cybersecurity, in line with the Dubai Cyber Security Strategy that is managed by DESC."

Certificate Authority Service for Dubai introduced by DESC

Dubai Electronic Security Center (DESC) will launch a dedicated Public Key Infrastructure and Certificate Authority (PKI/CA) service for Dubai government entities.

The PKI/CA will be established as part of Dubai's Cyber Security Strategy supporting DESC's vision, which hopes to make Dubai the safest electronic city in the world.

The Certificate Authority will issue digital certificates and public-private key pairs for Dubai's government entities. The main role of Dubai's Certificate Authority is to guarantee the authenticity and identity of the certificate holder, thereby facilitating numerous functions such as file encryption, secure communication channels and data exchange.

His Excellency Yousuf Al Shaibani, DESC Chief Executive Officer, said: "With the emerging trend of the Internet of Things (IoT), the rise of machine to machine communications, and the Dubai Smart City projects coming soon, it's becoming crucial to guarantee the authenticity of devices and people to ensure secure and safe communications between and among them."

The project is planned to be launched by mid of-2017, at which time Dubai government departments will be able to request and receive Digital Certificates.

DESC hosts Dubai Cyber Security Strategy Initiatives workshop

Dubai Electronic Security Center (DESC) has hosted its second workshop entitled "Dubai Cyber Security Strategy Initiatives" in support of the initial framework for the Dubai Cyber Security Strategy plan.

The workshop was held for the benefit of Dubai government departments to address the risks and challenges of electronic systems and government information. The Dubai Cyber Security Strategy aims to provide the world's safest infrastructure for e-service, which includes all government, semi-government and private sectors, including individuals such as citizens, residents and visitors.

During the workshop, the objectives of the plan were presented as was its main focus, which is to provide a secure electronic structure to counter the electronic challenges and build a society aware of the importance of electronic security. The executive plan was also presented to monitor the implementation of the objectives and performance indicators for each participating entity in the plan.

The workshop included creative and interactive discussions between participants to identify the challenges they face within their entities and within Dubai as a whole. This yielded a list of innovative ideas and solutions to overcome these risks with a set a timeframe for completion.

His Excellency Yousuf Al Shaibani, Chief Executive Office of DESC, said: "We are working with various organisations to develop deterrence plans for electronic security threats and challenges with high standards that will be implemented in coordination and cooperation between all parties in line with the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai."

Biggest cyberattack of all time impacts more than 100 countries

A ransomware attack, dubbed 'WannaCry' caused disruption to organisations and individuals across the world, as even the UK's National Health Service (NHS) was forced to cancel outpatient procedures in the wake of the strike.

Ransomware effectively shuts down a user's system, before demanding a ransom to be paid in order for the files and the system to be restored. In this case, the ransom was $300 per infected computer, and WannaCry was able to access systems due to the identification of an alleged defect in Microsoft Windows.

The tools for the attack were created and placed in the black market a month before the attack by a group of hackers known as the Shadow Brokers. Microsoft itself was aware of the vulnerability in its operating system, and as such it released an update which patched the security issue, but most organisations don't automatically update their software when it comes to Microsoft at it can often negatively affect other programs they use. The lack of awareness and urgency in updating systems and programs the moment one is made available has now impacted more than 200,000 systems in 100 countries.

The most high-profile organisations affected by the hack were FedEx, Nissan, Deutsche Bank, and the UK's NHS, while multiple Russian agencies and companies were also victims. It is the NHS, however, which exemplifies the impact such ransomware can have on the lives of people, even from a health perspective, as thousands of patients were unable to undergo treatment and some ambulances didn't even arrive.

Fortunately, after the high profile nature of the attack hit mainstream news channels, the infection did not spread, but form many the damage was already done. The identity of the individual hackers remains anonymous, although security experts have said they are most likely amateurs. Before the threat was curbed, the hackers had made just over $50,000.

Speaking of the WannaCry attack and its eradication, the UK government's cyber office said: "The way these attacks work means that compromises of machines and networks that have already occurred may not yet have been detected, and that existing infections from the malware can spread within networks."

Computer users are being urged to immediately perform updates to their systems and programs, where available, and remain cautious on clicking any links from an untrusted source received via email, Facebook, Twitter, or any other communication channels online.

New cybersecurity system inspired by the human brain detects attack 100 times faster

The Neuromorphic Cyber Microscope is able to search for complex patterns, instantly identifying security threats, all while using less power than a 60-watt lightbulb. The new system has been designed by Lewis Rhodes Labs, in collaboration with Sandia National Laboratories.

The majority of cybersecurity systems are programmed to search and identify general indicators of an attack, without having the capability to home in on specific patterns. It's a limitation that leaves the door open to the more advanced type of attacks designed to side step modern security measures and enter through the back door. But the Neuromorphic Cyber Microscope addresses that constraint, identifying specific threats directly, allowing security staff the reassurance that what has been identified constitutes a genuine threat.

Sandia tested the Neuromorphic Cyber Microscope on its cybertraffic in a demonstration environment against a conventional cybersecurity system, and the new system outperformed in every category.

The test showed it to be more than 100 times faster and 1,000 times more energy-efficient than racks of conventional cybersecurity systems. The Neuromorphic Cyber Microscope is in the early stages of deployment.

Smart phone users lack security awareness

A report issued recently by Pew Research Center has revealed a concerning lack of security awareness among smart phone users. The most basic security measures call for the user to use a pass code and update both the apps and operating system regularly, and yet a surprising amount of users do not adhere to any of these best practices.

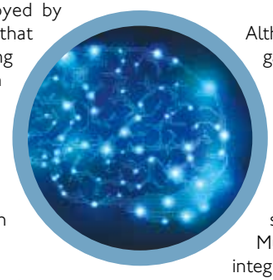
The research found that 28% of those interviewed do not use a pass code for their smart phone, while 40% say that they do not update their apps or operating system often – choosing instead to do updates when it's convenient for them. 14% never update their operating system, while 10% elect not to update apps. Although only 3% said they never use a pass code or update anything on their smart phones, only 22% do all of these. The majority (75%) fall into the middle category of the mobile security spectrum.

This group use a screen lock but only update their phone's apps and operating system when it's convenient for them to do so. In terms of age groups, owners aged 65 and older proved much less likely than adults younger than 65 to use a screen lock and are also more than twice as likely as younger users not to take any of the suggested best practices to secure their phones.

In addition, the kinds of actions carried out on smart devices are also a cause for concern. 54% of smart phone owners reported using public Wi-Fi networks, while 20% admitted to having performed internet banking or online shopping while using these insecure networks. One of the biggest threats to personal information breaches is the use of networks at malls, airports or in cafés and restaurants.

Elon Musk to combine brains with computers

Elon Musk has revealed via his Twitter account that he intends to start a new tech company called Neuralink. This venture will be dedicated to the creation of a brain/computer interface, and seems to have been buoyed by his well-publicised concerns that Artificial Intelligence is advancing at such a rate that it may soon surpass human existence, and effectively take over the world.



In his tweet, he said it's "difficult to dedicate the time, but existential risk is too high not to."

Neuralink will create devices that can be implanted into the human brain, creating "meta-humans" of superior intelligence and processing levels that could potentially stave off the rise of the machines. In Dubai at the World Government Summit, a segment of his appearance was dedicated to talking about this concept.

Although Musk's ventures will garner the headlines, others are also working on something similar. The US Defense Department is one such organisation, but much of the work carried out by their research arm is very secretive. More is expected on Musk's plans for human/machine integration shortly, although finding time between SpaceX, Tesla and the various other ongoing projects he has, could be the biggest challenge for the billionaire tech visionary.

Dubai Police warn of severe punishments for cyber criminals in the UAE

The World Wide Web is a vast phenomenon, and thanks to the spread of social networks, cybercrime is growing steadily, and people across the world become victims of different hacking techniques on a daily basis. Hacking attacks are perpetrated for several reasons, including invasion of privacy, theft and impersonation. All these attacks are done through phishing links and fake web pages.

His Excellency Major General Expert Khalil Ibrahim Al Mansouri , Assistant Commander of CID at Dubai Police, tells us that the internet has positive and negative effects, and with the spread of online social networking, which can now be accessed directly through mobile phones, a channel for hackers to hack into victims' computers for the purposes of blackmail has been created.

Al Mansouri said that children under 18 years of age are the most vulnerable to hacking attacks, because they do not know how to protect their email or social network accounts.

Types of hackers

Al Mansouri points out that there are hackers who deliberately target girls and use their private information to blackmail them. "There are others who collect information to commit fraudulent activities. Some hackers use phishing scams and others attack specific targets by using the information they obtain for blackmail or extortion purposes. There are also hackers who work within cyber-based crime gangs," he tells us.

"Hackers use phishing scams to send users links that are supposed to take them to a trusted site, where they are asked for their personal or financial information. The reality is they are taken to a rogue website."

Hacking Techniques

There are a variety of methods used in carrying out attacks on computers and phones, Al Mansouri says. "Hackers can attack in so many ways, including using spy software that grants them access to files saved on a desktop, or sending links that enable them to access users' pictures and messages to blackmail them."

He warns users from opening applications promoted on WhatsApp groups created for the purpose of spying.

Al Mansouri says that school and university students are the most vulnerable to online blackmail because they are not familiar with social media sites and are unaware of the importance of updating their devices. Most of them store their pictures in their emails or social networks, but do not activate the passcode feature or the 'find my phone' feature on their devices. This makes their phone vulnerable to hacking or even theft, which leads girls to becoming victims of blackmail and exploitation.

Al Mansouri said that the Cybercrimes Department at Dubai Police has a team of female police officers that take victim statements confidentially in the presence of their parents.

Providing protection and raising awareness

Email security is important to protect users from hacker attacks and falling victim to blackmail. Therefore, Lieutenant Colonel Salem bin Salmeen, Deputy Director of the Cybercrimes Department at Dubai Police, provides some useful tips in this regard:

"Use trusted security software and set it to update automatically. Do not click on links within unknown email messages. Check your security and privacy policies on social network sites and link them to a phone number and another email address," he tells us.

> Some hackers use phishing scams and others attack targets for blackmail or extortion purposes. There are also hackers who work within cyber-based crime gangs

HE Major General Expert Khalil Ibrahim Al Mansouri

> Dubai Police aspires to raise awareness on the risks of cybercrimes

Lieutenant Colonel Salem bin Salmeen

The Cybercrimes Department at Dubai Police has held a number of lectures and public awareness programmes targeting school and university students as they are the group who use social media the most. Furthermore, Dubai Police creates numerous campaigns to raise awareness in both Arabic and English, provides tips on its official Twitter account, and holds lectures in the Majalis to raise community awareness on the risks of cybercrime.

Salmeen urges anyone who has been fallen victim to cybercrime to report the incident to Dubai Police using communication channels or calling: 800CID (800243).

The psychology of hackers

Psychologist Mohammad Al Nahas also spoke to us, and describes the psychology of hackers, saying: "Hackers are highly intelligent, however they use their intelligence and skills to invade people's privacy in order to intrude upon, blackmail or extort them. All hacking incidents should be reported, as it is morally wrong and against the law."

Al Nahas said that any hacker who attempts to abuse and exploit children on the internet is a psychopath who enjoys hurting others. This person may have been abused as a child and chooses to engage in crime to seek revenge against society.

Al Nahas warned families that children can escape from parental supervision, no matter how strict this supervision is, because the internet is available to everyone and it is very hard to control or monitor child activities online.
He also stressed the importance of promoting self-confidence in children by providing them the right information and explaining to them the risks of misusing social media.

Penalty is up to one million Dirhams

Emirati advocate Yousef Albahar praised the role played by the UAE legislators in addressing the hacking issue which has negatively affected human rights and has generated crimes like fraud, blackmailing and other crimes of a similar nature.

To prevent hacking, Article No. 2 of the Federal Decree Law on Combating Cybercrimes provided harsh penalties, stating that the perpetrator(s): "Shall be punished by imprisonment and a fine not less than AED 100,000 and not in excess of AED 300,000, or either of these two penalties, if they have gained access to a website, an electronic information system, computer network or information technology means without authorisation or in excess of authorisation, or if they unlawfully remain therein."

So, whoever gains access to a website without authorisation shall be punished by imprisonment and receive a fine of not less than AED 100,000 and not in excess of AED 300,000. The fine and the period of imprisonment are up to the court to determine depending on the severity and seriousness of the cybercrime. This deterrent penalty comes in line with the UAE legislators' belief of the importance of protecting privacy.

In case of deleting, destroying or publishing any personal data or information, section (3) of this Article increases the penalty to imprisonment for a period of at least one year and a fine of not less than AED 250,000 and not in excess of AED 1 million, or either of these two penalties.

Also, whoever accesses websites without authorisation to obtain government data, or confidential information relating to a financial, commercial or economical facility shall be punished according to Article No. 4 of Federal Decree Law on Combating Cybercrimes by temporary imprisonment which ranges from three to 15 years according to the court and a fine of not less than AED 250,000 and not in excess of AED 1.5 million.

> No matter how strict parental supervision is, children can escape it; the solution is to provide them with the right information

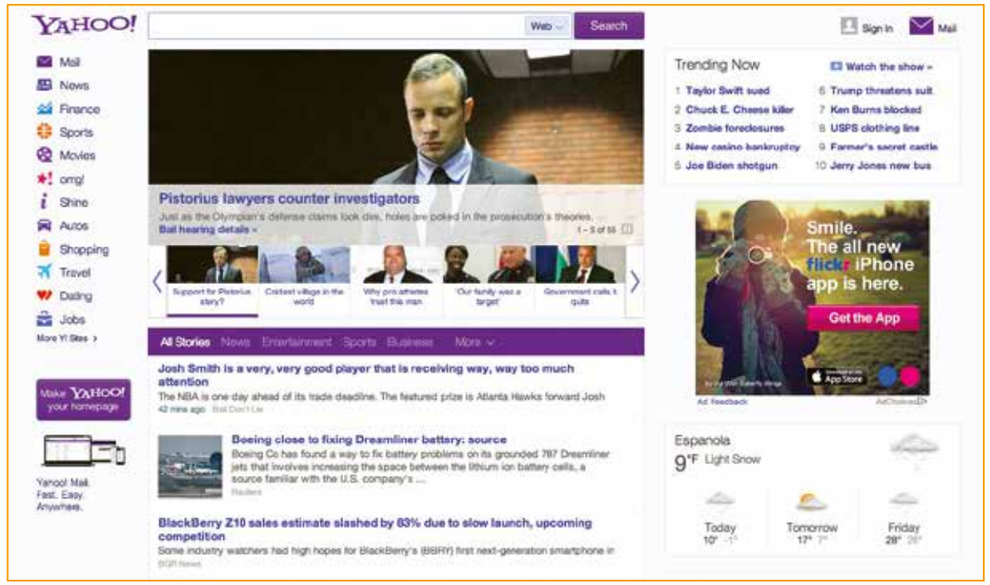
Mohammad Al Nahas, Psychologist

> The UAE legislators are aware of the importance of protecting privacy, and the laws provide for harsh penalties

Yousef Albahar Lawyer

The one click Yahoo! hack

As the FBI closes in on the suspects in the Yahoo data breach, Esharat looks back at the details of one of the largest scale hacks in history – kept secret from the public and its customers for two years for fear of relinquishing an already uncertain user base.



It only took one employee's negligence to open up one of the largest multinational tech companies in the world to a team of hackers. Yahoo's internal networks were left wide open, after the most basic of attempts at spear phishing.

Phishing attacks have become more advanced in recent years, as now a link can be cleverly hidden within social media sites, or even genuine-looking websites with similar Url's to the genuine article. But the Yahoo attack was accomplished with a simple and somewhat speculative email campaign containing a link. It takes only one click to carve open a massive hole, even in a tech giant's network. And this click was to become the biggest data breach in history. Here's what we know about the big one click Yahoo hack:

The alleged masterminds behind this 2014 attack were officially charged with the cybercrime just one month ago. Their crime was to hack and compromise 500 million Yahoo user accounts.

As a result of the charges, more has now been revealed about the 2014 hack, which began with a spear phishing email sent to semi-privileged Yahoo employees. The top level executives were not targeted. Nobody knows exactly how many Yahoo staff received the email, but what is known, is that at least one of the targets clicked on the link contained within it – and that's all it took to grant access to the hackers.

Alexsey Belan, who was already on the FBI's Most Wanted Hackers list, was now inside the Yahoo network, and he found two key assets worth a great deal to his employers. The first was the Yahoo User Database, containing personal information about all the Yahoo users. Next was the Account Management Tool, which was used to edit the database.

Belan used a File Transfer Protocol (FTP) to download the entire database. Inside, he found more information than he could have hoped for: usernames, phone numbers, security questions, security answers, password recovery emails and the cryptographic value for each account.

With the last two components, Belan and Baratov had access to the accounts of all the users they were told to hack by their employers. They were able to search the users by their recovery email addresses, and then were able to generate forged access cookies for the accounts, so their employers were able to access the email accounts without the need for a password.

The FBI says that between 2015 and 2016, these cookies were generated numerous times, and that 6,500 Yahoo accounts were specifically targeted – of the 500 million available. Some of the accounts compromised belonged to politicians and dignitaries, journalists, officials of states, government officials and airline employees, amongst others.

The FBI reports that Yahoo first approached them in 2014 about the hack, which suggests it didn't go unnoticed for long. But the organisation didn't allow the data breach to become public knowledge until December last year, when they advised hundreds of millions of Yahoo account users to change their passwords.

While it appears that the targets of the hack were individuals with potentially significant information to the hackers, there are 500 million Yahoo accounts with usernames, passwords and other personal information that will most likely be made available to other hacking groups keen to get going on a phishing scam of their own - potentially targeted at financial information. For the millions of Yahoo customers affected, extra vigilance and password changes are well advised; for Yahoo, $200 million was wiped off its selling price to Verizon as a result of the hack - a costly error by a staff member.

Igor Suschin, Dmitry Dokuchaev
Aleksey Belan and Karim Baratov

Innovator Ahmad Al Hammadi wins the Pan-Arab ALECSO Grand Competition

Ahmad Al Hammadi made his country proud when he beat 56 participants from 19 Arab countries and took first place in the pan-Arab ALECSO Grand Competition for 2016. He was awarded the first place for developing an innovative mobile app dubbed the "Smart Museum". This app enables its users to virtually visit museums and view their exhibits by using advanced techniques.

Another great innovation of Al Hammadi – with which he broke into the defence industry – opens the door to various military training activities. This innovation was showcased at the International Defence Exhibition, IDEX. Moreover, Al Hammadi intends to enter the oil business with an application that allows its users to virtually walk around oil fields. To talk about his innovations, Esharat met Al Hammadi, who is pursuing a Master of Science degree in Information Technology at ADU. We asked him the following questions:

Esharat: What is the nature of your new innovation showcased in the International Defence Exhibition, IDEX, in Abu Dhabi?

Al Hammadi: "I developed an application for the purposes of professional military training using Microsoft HoloLens. It allows the user to visualise a virtual object mixed in real world and to move naturally around it.

"The application features a virtual war plane, bombs and firearms that appear to users when they wear the HoloLens. They can move around the plane to explore it and view the firearms using voice commands."

Esharat: How important is your participation in this major exhibition?

Al Hammadi: "IDEX is one of the largest international defence exhibitions dedicated to military defence systems. It demonstrates the latest technology. I participated with a new technology that was showcased for the first time; all those who tried out the HoloLens were very interested and wanted to incorporate it into their training programmes. This technology enhances the way trainees absorb information, as it enables them to visualise the internal components of weapons in front of them. It also saves the trainer the trouble of physically showing the equipment to the trainees."

Esharat: Your application has been awarded first place in the science category of the ALECSO Grand Competition for Mobile Apps for the year 2016. What does winning mean to you?

Al Hammadi: "As I represented the UAE in the competition, I felt that it was more like a national accomplishment rather than a personal one. What made me even more proud is that this is the second consecutive year I've won the award, as I won in the Education category of the first edition of

the competition with an application called "Droosy", which aims to help students study and manage their subjects."

Esharat: What is so special about the "Smart Museum" application, and what is its purpose?

Al Hammadi: "It is an application that utilises augmented reality and 360-degree technology to enable users to virtually visit museums and view exhibits. This application rules out the need to travel to visit museums. It also offers a perfect opportunity to learn about museums and artefacts. Thanks to the technology of augmented reality, the user can get detailed information about any artefact just by pointing the smart phone's camera towards it.

"The purpose of this application is to preserve the history of Arab culture using modern technology that keeps abreast of the rapid technological developments, as well as deepening users' knowledge of artefacts and museums around the world."

Esharat: What are the museums covered by the application in the UAE?

Al Hammadi: "The application covers 19 museums; namely the Horse Museum, Saruq Al-Hadid Archaeology Museum, Museum of the Poet Al Oqaili, Coin Museum, Camel Museum, Qasr Al Muwaiji, Qasr al Hosn, Al Jahili Fort, Sultan Fort, Sheikh Saeed Al Maktoum House, Majlis Ghorfat Umm Al Sheif, Diving Village, Jumaa and Obaid bin Thani House, Heritage Village, Heritage House, Al Fahidi Historical Neighbourhood and Al Ahmadiya School.

"The application also uses the technology of augmented reality to cover the Zayed National Museum in Al Bateen district, Abu Dhabi near ADCO."

Esharat: The Hayak application for the Securities and Commodities Authority (SCA) is your first innovation as a student of Higher Colleges of Technology. Talk us through it?

Al Hammadi: "Hayak is an online onboarding system that I developed for new SCA employees when I was a student. With this app, new employees can learn about SCA using an innovative and interactive video technology. The application asks a new employee a group of questions that are relevant to a specific department, then moves to the next department and so on until the employee finishes all the departments, and then he/she can start working in about an hour.

"Hayak saved a lot of time for SCA, given that the orientation process used to take a week in the past."

Esharat: What advice would you give to the Emirati youth?

Al Hammadi: "My advice to technophiles is to keep abreast of the latest technology, try everything out, and participate in exhibitions and conferences showcasing new tech. This will allow them to obtain exposure and experience from around the globe and find out about the latest discoveries in science and technology.

"As for the youth in general, I advise them to opt for creativity and innovation in their lifestyle choice, so as to continue our journey to progress and success."

Esharat: Are you currently working on any new inventions or innovations?

Al Hammadi: "I am working on a special application to be used with Microsoft HoloLens. It will display entire oil fields. The purpose of this application is to provide training to staff without having to be physically on the field.

"This application is part of my Masters thesis, which is about virtual education. I am also developing an application for Abu Dhabi Tourism & Culture Authority to show the landmarks and sights of Abu Dhabi with the goal of promoting tourism in the UAE."

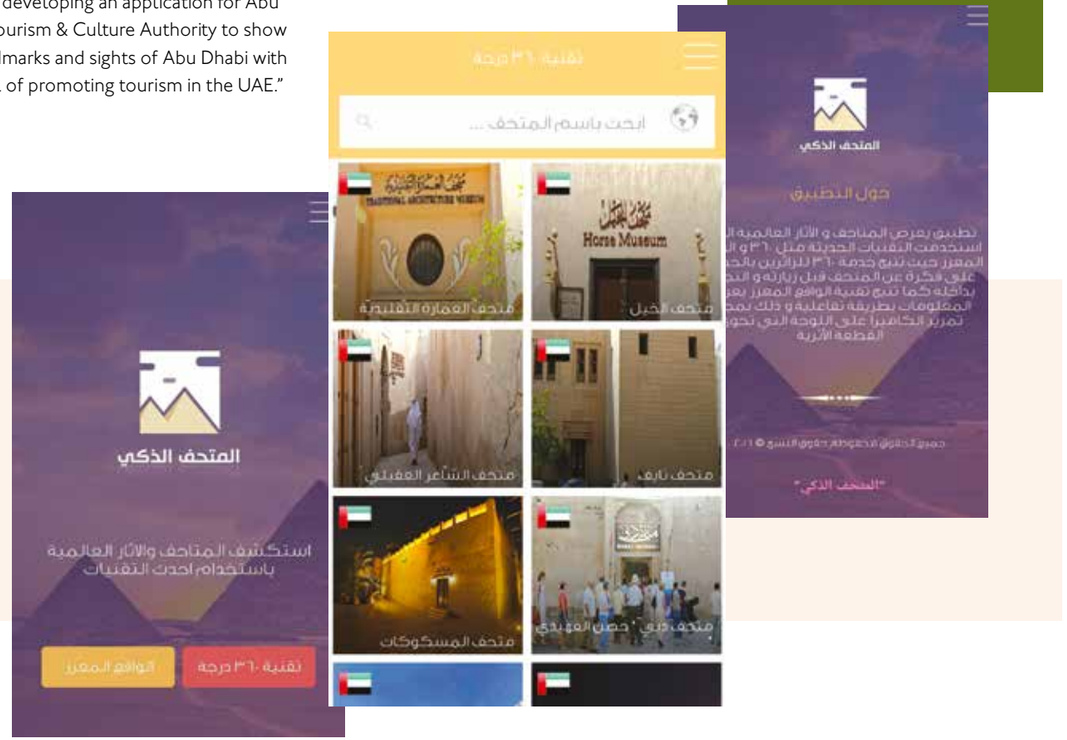
Esharat: Will you consider releasing another version of the "Smart Museum" app to cover other landmarks?

Al Hammadi: "I started working recently on the technology of the "Smart Museum" app for the benefit of Sharjah Museum of Islamic Civilisation, as well as cooperating with entities concerned with cultural heritage in the UAE so that the application becomes an integrated database of all national museums.

"Furthermore, I started gearing up for the third edition of pan-Arab ALECSO Mobile Apps Award that will be held in Tunisia."

Esharat: What do you aspire to do in the future?

Al Hammadi: "I aspire to become a key player in the IT sector and harness all that I have learned to serve my country."



Kevin Mitnick: "Nothing is unhackable"

Kevin Mitnick is a leading American computer security consultant, author and hacker. He is perhaps best known for a high-profile arrest in 1995 which led to a five-year prison sentence for numerous computer and communications-related crimes.

His arrest and trial, as well as the initial pursuit and the coverage in the media courted much controversy at the time, but he has put that chapter firmly behind him and is now one of the most famous and successful figures in cybersecurity globally

> Social engineering is using manipulation and deception to get a target to comply

Kevin Mitnick runs Mitnick Security Consulting, a security firm that helps large organisations identify potential loopholes and weaknesses in their security procedures. He is also an adviser to the very government that once saw him as a national security danger, using his extraordinary hacking capabilities for the greater good, rather than mischief that inevitably ends up in the authorities getting involved. If he were able to advise the government back 20 years ago during his own case, he may have avoided solitary confinement in prison, as much of the hysteria surrounding his hacking potential was frankly overblown, he says.

"20 years ago when I went to court, a federal prosecutor told the judge I was such a grave danger to national security that they had to make sure I couldn't access a phone while in prison, because I could dial up to NORAD (North American Aerospace Defense Command), connect to their modem and launch a nuclear weapon. I started laughing because I'd never heard of something so ridiculous. But the judge believed this and so I was put in the hole for a year," he tells us.

Fast forward 20 years and the world is a very different place. But, while dialling the number of a military institution and gaining the nuclear codes from a prison phone might seem a little far-fetched, similar acts are not entirely beyond the realms of possibility, even in 2017. When it comes to nuclear clearance however, it's remote, and unlikely.

"Similar acts are possible. It's called social engineering," Kevin says. "Social engineering is using manipulation, deception and influence to get a target to comply with a request. For example: I could send you a text message and make it appear as though it's anybody that I want.

"If somebody wants to steal the financials from a company, an adversary – a hacker – could send a message to the CFO's executive assistant, pretending to be from the CFO. It could say: 'When Kevin calls, please go ahead and release those third-quarter financials. By the way, don't text or call me because I'm in an important meeting. What are the chances that the executive assistant is going to follow through and give me complete access?" he asks.

According to Kevin, the chances are high, and similar plots are successfully carried out on a daily basis. Seemingly it's not only computer systems that are fallible, but also staff members who take a lackadaisical approach to security awareness. They often provide the entry point for hackers.

Kevin says nothing is unhackable; no system, no smart device, no email address, and no person. However, he says, if you do not wish for external parties to view your communications, whether on phone or pc, the answer is encryption. WhatsApp recently caused a stir among certain governments that claim terrorism can be countered if the world's most popular messaging platform would only de-encrypt the communications sent over its network and give them full access. Users of the service are not so sure, and Facebook (the parent company of WhatsApp) has held firm over this issue.

"It's all about end-to-end encryption, and there are apps for smart phones that offer this secure method. Encryption keys are placed upon your device and the person that you're communicating with. Some network providers don't allow this though, and you do wonder why," he says.

"But what it means is that if a hacker or a law agency wanted to intercept your communications, and this goes for WhatsApp too (banned in 12 countries because of the encryption, privacy and security it offers users), they could only do this by getting malware on your device. But they couldn't actually monitor the communication and decrypt it," he continues.

It's Kevin's job to make sure that his clients are prepared for whatever may come their way. And he does this job for governments and private entities across the world, depending upon which solution they request.

He tells us: "We still hack into systems, but it's not to do anything counter-productive or compromising, it's for the sake of security testing. So companies from all around the world hire my company to try to break in to businesses by exploiting technological flaws, by manipulating people, by getting in physically and also by getting in through mobile phones."

How aware are the governments of the world about how seriously they need to take the threat of cyber attacks? According to Kevin, they are very aware, as many approach his company daily to ask for his support and services.

"Even yesterday I was contacted by a third party contractor of a foreign government to seek out zero-day exploits on their behalf. Zero-day exploits are flaws in the security of software that haven't been fixed or even identified by the developer. We also got approached to enquire as to whether they could buy cyber weapons from us that they could use at their discretion. But we don't deal with foreign entities when it comes to zero-day exploits. We don't even discuss it," he says.

Controversy even spilled over into the Presidential elections in the US, which, it is claimed, was compromised by hackers breaching voter databases and potentially costing Hilary Clinton the Presidency. And it's not the first time elections are said to have been the target for a cyber attack to influence an outcome.

"It's already routine. In this case, the United States Government has pointed the finger at Russians for hacking into the Democratic National Committee. It's a bad thing to be compromised. Governments, private and public sector businesses need to have better security - and that's really the bottom line.

> Individuals have to take the reins and start exercising due diligence

"And you know, most companies are getting hacked - and it starts with just an email. Then the bad guy gets full control over that computer. And then at that point they could laterally move inside the network.

"An attacker could send a target a PDF file and gain full control of a computer; We just need to raise awareness, and to encourage people and organisations that they really need to re-think their defences and do something pro-actively to prevent becoming the next victim," Kevin tells us.

But what can organisations, and particularly us as individuals do, especially if, as Kevin says, nothing is unhackable and if somebody really wants to access your system, and if they have the resources and the finances available, they will anyway?

He finishes by saying: "Individuals and businesses need to know that they can't depend on their respective governments to protect them. What they have to do is take the reins into their own hands and start exercising due diligence. Rather than being reactive, be proactive: layer their defences and make it really hard for a hacker or any other type of adversary to get into the network. And that's what is important."

ICAO stresses need for cyber resilience

Every nation should assess the risk that cyber terrorism poses to its civil aviation industry, build its own capability to address such threats and ensure that the laws that govern such crimes are fit for purpose, according to the global aviation industry leadership.

The call was made at the inaugural Cyber Summit convened by the International Civil Aviation Organisation (ICAO) in Dubai which concluded by issuing an industry declaration on cybersecurity. The forum discussed emerging cyber risks to the industry that were the subject of a resolution at the 39th ICAO Assembly. This similarly sought ways to mount a strong industry response to the proliferation of cyber attacks.

His Excellency Saif Al Suwaidi, Director General of the General Civil Aviation Authority, said: "Ensuring cooperation between government entities, the international aviation industry partners and the multitude of stakeholders who are fundamental in combating cyber threats is crucial."

"Collaboration and exchange between states and other stakeholders is the sine qua non for the development of an effective and coordinated global framework to address the challenges of cybersecurity in civil aviation," the declaration stated, adding: "Cybersecurity matters must be fully considered and coordinated across all relevant disciplines within state aviation authorities.

"Therefore it is imperative that all states and ICAO work to ensure the early entry into force and universal adoption of the Beijing Instruments, as called for in the Beijing Convention and Beijing Protocol of 2010," the declaration added.

Cybersecurity: 10 tips for protecting against cybercrime

Professional hacking is the art of successfully tricking a person initially, and then using the information provided to you for personal gain – damaging the individual in the process. But although the world is more tech-savvy and guarded against hacking than it ever has been, the hackers have also become more advanced. It's an on-going battle, but you can reduce your risk of falling victim to a phishing scam, or infecting your computer with malware, by following these 10 tips for protecting yourself from cybercrime:

1 Be extra vigilant on social media

For hackers and scam artists, social media is their utopia. Breaches through social channels have increased exorbitantly in the last five years, and an indifferent approach to sharing information is what leaves you wide open to becoming a victim. Remove your home address, phone number, date of birth and any other information that could be used to fake your identity. Many also choose to delete or edit "likes" and groups, while hiding friend's lists. The more hackers know, the more convincing a phishing email they can spam you with. Change your privacy settings to the most private possible, limit access to an inner circle of family and friends, and never share personal information with any people you meet online.

2 Don't use debit cards online, use credit cards

Unauthorised debit card charges are taken directly from your bank account, and even if you report the breach immediately, it could take weeks for stolen money to be recovered, if it even is at all. By using a credit card online, you are provided an extra level of protection not afforded by banks and debit cards. Visa in particular is a leader in secure payments and transactions, and will often spot suspicious transactions without the need to contact them. But despite the credit card giant providing excellence in transaction security, there are things you should never do when paying online. Never store your credit card details for future use. One data breach for the organisation with which your details are stored and you could be facing a huge loss. It doesn't happen often, but it does happen. Typing in your credit card details just takes an extra 60 seconds.

3 Always use two-step verification

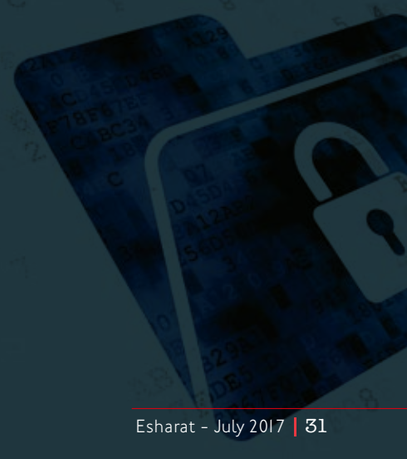
Your email or cloud service should offer two-step verification for logins. Use it. Facebook and Twitter also provide this valuable security function. A hacker may be able to work out your password, but they can't access your account without the unique verification code that gets sent to your phone every time a login is attempted from a different device.

4 Be aware that Apple Macs are now just as susceptible as PCs to viruses

Steve Jobs, for all his genius, was not commander of an invincible, unhackable operating system. So while it was perhaps once true that Apple products were not often the victim of malware, that was only because next to PCs and the Windows OS, hackers thought creating Apple hacks to be a waste of their time as user numbers were so insignificant. That's not the case now, and as such a good number of hackers primarily target the Mac community. Be aware regardless of what OS you're using.

5 Use anti-virus software

Everyone should use anti-virus and anti-spyware programs to remove or disarm viruses at the front door. Ensure your anti-virus program is always updated to the latest version; you can set this up to automatically happen. Some programmers are not fans of anti-virus software, claiming it to be responsible for slowing down systems, but infected systems run a lot slower, and are also wide open to data breaches. Security is more important than super speed.



6 Look closely at the URL

If you receive an email or you are looking at a hyperlink somewhere on the web, take a really good look at the URL. The name of your bank or a very reputable institution may well be incorporated into the URL, and when you get to the site it may be a perfect copycat of the genuine site, but using this site will open you up to a breach and personal loss. Examples of fake URLs can be if the bank name is slightly misspelled, or if instead of the URL: www.bank.com, it appears as www.bank.money.com. No bank uses URLs like this. In the end, anything that looks remotely suspicious needs to be approached with caution.

7 Ignore emails requesting personal information

Nowadays, phishing scams have become far more advanced than the poor efforts of a decade ago. Gone are the "You have won $4,500,000 dollars in the local lottery draw, please send your bank details to receive the monies…" and they have been replaced with fake bank emails or requests to update personal information from what would appear to be a genuine site. But no reputable bank or organisation will ever request any information via email. If you're still convinced the email is genuine, simply check the email address of the sender - it won't be an email that suggests it was sent from an employee of the organisation. Avoid at all costs.

8 Careful with public Wi-Fi

Public Wi-Fi is a hacker's dream. It is more often than not un-encrypted and completely unsecure. Once data leaves your device headed for a web destination, it can be intercepted. It's not a good idea to ever bank online on a public Wi-Fi network.

9 Different passwords, different email accounts

It should go without saying that a different password should be in place for all the different accounts you have. But still it's not uncommon to find users with the same password for everything - from online banking to Facebook. This is a big mistake. Also something to be aware of is the requirement to have different email addresses in place for each facet of your virtual life. One email address registered with online banking, one for socials, and another for online shopping is advisable. It means that everything is kept separate, and if one email is compromised or hacked, the others remain intact. The same email address for everything is a treasure trove of information for a hacker – financial details, passport info, addresses, phone numbers etc.

10 Don't click on links, or pop-ups unless they are 100% from a trusted source

Remember that your behaviour online is monitored thanks to social media and more advanced algorithms that watch all you do. This information is available to hackers, so if you're an online shopping addict, you can expect to be targeted with online ads trying to convince you to buy something similar to what you've bought previously. But pop-ups can contain malicious software that tricks a user into verifying something. Ignore pop-ups offering things like site surveys on e-commerce sites, as they are sometimes where the malcode is. Hackers infect PCs with malware by luring users to click on a link or open an attachment. They know what you're interested in, and can send you customised messages, inviting you to click on something which looks appealing.

Exposed! Computer virus myths and misconceptions

There are many common mistakes when it comes to understanding viruses and malware – in terms of the cause, the cures and the long term effects. Esharat examines some of the biggest myths on computer viruses…

1 A firewall protects from viruses

A firewall doesn't protect a computer from spyware, trojan or a virus. In terms of malware, it will protect from a worm, because they use the network to travel. A firewall will also alert you when malware is sending data from your system back to their authors, but by then, the malware is already infected.

2 Viruses damage hardware

No they don't… A virus affects software, not hardware. Worst case scenario you'll need to wipe or replace your basic input/output system in your firewall, but that's still not hardware.

3 If a computer is flashing up errors all the time, it has a virus

Definitely not. A file can become corrupt very easily through a bug, and impromptu restart, faulty hardware or software, the list goes on…

4 Reinstalling Windows and copying the files back will solve everything

If a virus has infected your computer, just reinstalling Windows and re-uploading all your files will just re-infect your computer. Before reloading your documents and files, they need to be scanned for corrupt files.

5 Anti-virus programs are always right

False. Particularly when it comes to downloading files from the web. Some Anti-virus programs will block perfectly legitimate downloads because of a supposed virus – despite there being no virus at all. The best way to scan the legitimacy of a file is not to rely upon your anti-virus software, and instead to scan online using VirusTotal.

6 BSOD equals virus

The Blue Screen of Death (BSOD) is feared by all computer users. But it seldom means for sure that a virus is present. The BSOD is usually caused by faulty hardware. The best practice is to take a note of the error code and let Google do the work for you.

7 Smart phones don't get viruses

The majority of viruses, it is true, are authored to exploit computers. But this is because traditionally computers were all anyone really used. But the popularity of smart phones has grown markedly in the decades since the internet became more than just a dial-up novelty to the mainstream. And so the smart phone market is now on the radar for hackers. Smart phone malware is on the increase. All platforms are susceptible. Be vigilant regardless of what you use.

Identity theft could you be a victim?

According to the 2017 Identity Fraud Study released by Javelin Strategy & Research, researchers estimate there have been more than 50 million cases of identity theft in the last 10 years. But although it is a growing criminal activity, identity theft is still a crime which many of us don't take seriously. We tend to take the approach that "it will never happen to me…" and "why would anyone want my identity?"; these are dangerous approaches.

If an identity thief manages to get hold of your personal information, the results can be life-changing for the individual. The overall effects range from the emptying out your bank account and maxing out your credit cards, to giving your name in case of an arrest and travelling between countries using a passport in your name.

Signs your identity has been stolen

There are some tell-tale signs that you have been targeted by an identity thief, for example:

- Your bank statement shows withdrawals you didn't make.
- You have ceased to receive bills from credit cards or utilities.
- Your cheques begin to bounce.
- Your medical insurance shows up as having been used when you know it hasn't been.
- You receive information that a data breach has occurred within an organisation that held your information on their system.

What to do?

If you notice that somebody is impersonating you and opening up credit cards, store cards or attempting to get bank accounts and loans in your name, you should immediately contact the Police and also the concerned organisations to inform them of the situation.

Having your identity stolen is not a pleasant experience, and sometimes will involve a protracted process in order set things right, but a failure to react immediately if you suspect someone has assumed your identity will lead to further complications in the long run.

Remember: always be vigilant, always check your statements for unusual activity, and most of all, guard your personal documents, information and cards.