ISSUE 03 FEBRUARY 2019

إشارات Esharat

Dedicated to a safer cyberspace

SHEIKH MAKTOUM SUPPORTS THE PROGRESS OF BLOCKCHAIN IN DUBAI

ONLINE PUBLISHING LAWS PROTECT SOCIAL COMMUNITIES

HOW SAFE ARE YOUR CHILD'S VIDEO GAMES?

DESC IS THE RELIABLE SECURITY PARTNER OF ALL GOVERNMENT ENTITIES IN DUBAI

DESC LICENSING FOR CYBERSECURITY FIRMS WILL BOOST CONFIDENCE AND GROWTH IN THE SECTOR

Let us all stay SAFE, SMART & SECURE on social media

Social media channels allow us to share information among friends and family members as well as wider audiences, such as government entities, companies, even celebrities and individuals we do not know personally. In the midst of this wide range of e-content, DESC urges you to stay safe on social media with the following tips:

- Always configure your privacy and security settings on all your accounts.
- Ensure you have a strong and individual password to each of your accounts.
- Avoid sharing your personal information, like your phone number or daily routine, which will make you vulnerable to theft.
- Be especially wary of strangers. Think twice before accepting friend requests.

Never forget that the internet is an open gate to the digital world and every log-in leaves a trail of data that makes you unintentionally vulnerable online.

مركز دبي للأمن الإلكتروني
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

www.desc.dubai.ae

Editorial and Design
7G MEDIA

Editorial Board
Amani Abuseedo
Nicole Rehbane
Mary Jane Botha
Ahmed Mersal

Design and Production
Sree E S
Aws Rahhal

Illustrator
Joseph Cartaño

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

All content provided by Esharat magazine is for informational purposes only. Although every reasonable effort is made to present current and accurate information, Esharat makes no guarantees of any kind and cannot be held liable for any outdated or incorrect information.

INSIDE

Supporting the vision

The massive digitalization of the 21st century is all-pervasive and inevitable. Dubai's leaders have chosen to remain technologically informed, open to all the astonishing possibilities of the cyberworld as well as its challenges.

By embracing these revolutionary changes, the wise leadership of Dubai is enabling previously unimaginable progress, efficiencies and convenience - helping to create a better life for all who walk the Emirate's busy city streets. This intensive technological impact requires judicious and resourceful management, a mandate that the Dubai Electronic Security Center (DESC) is honored to accomplish.

The aspirations of technological development require a support system of incisively structured frameworks to ensure the security of the massive information systems in which they operate. In this regard, DESC's strategic plans not only promote and enhance Dubai's cyberwealth but also protect Dubai's cyberspace from subversive attacks and crime by ensuring that the level of electronic security is of top-level international standards.

Since its inception in 2014, DESC has initiated and managed the digital transformation and technological advancement of all government entities within the Emirate. The Center's initiatives, most prominently the Dubai Cyber Security Strategy, launched in 2017 by Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, are helping to establish Dubai as a global leader in cyber innovation, safety and security.

Most recently, DESC has partnered with the Department of Economic Development to introduce trade licenses for companies offering cybersecurity-related services. For this reason, DESC's official certification serves to verify the integrity and internationally regulated skills of the cyber service provider, thereby strengthening the development of this fast-growing corporate sector.

DESC optimizes continuous progress of the UAE's cybersecurity landscape by encouraging innovative solutions that will keep the region ahead of the game, positioning itself at the forefront of global dialogue and supporting expert events such as the IEEE UAE Cyber Intelligence Summit.

This issue of Esharat is full of informative articles that highlight the robust support that DESC brings to this celebrated city and its far-thinking leaders, as well as some easy tips and interesting articles to help you stay informed and enlightened about the exciting world of cybertechnology.

Yousuf Hamad Al Shaibani

Director General
Dubai Electronic Security Center

HH Sheikh Maktoum, at the Future Blockchain Summit 2018: "UAE will always be a pioneer in science and technology"

His Highness Sheikh Maktoum bin Mohammed bin Rashid Al Maktoum, Deputy Ruler of Dubai, welcomed delegates to Dubai's 2018 Future Blockchain Summit, the first ever experiential conference of its kind hosted by any city.

Speaking at the Future Blockchain Summit's opening session, Sheikh Maktoum Al Maktoum welcomed participants and stressed the importance of hosting such forums and dialogues in the UAE. He stressed that active collaboration strengthens the country's international position on the economic, tourism and international technology maps. It also enriches scientific and technical expertise, and provides opportunities for Emirati youth to learn about innovations, supporting the UAE's pioneering role.

The important inaugural event was held at the Dubai World Trade Centre, with over 7,000 senior government advisors, international industry leaders, technologists and future strategists gathered to discuss the challenges of the future and ways to accelerate blockchain application in Dubai and further afield.

Realising the future today

Featuring more than 70 sessions, the Future Blockchain Summit focused on moving beyond technological theories to examine the feasibility of real-world applications for blockchain across a broad reach of sectors. These include energy, retail and e-commerce, banking, transportation, healthcare, security and education.

Expert participation

The 2018 Future Blockchain Summit included closed-door briefings on regulations and case studies, active participation workshops on the technology and exciting exhibitions from a wealth of blockchain-related stakeholders. Prominent speakers at the Summit included entrepreneurs at the cutting edge of blockchain development, such as Dr Larry Sanger, co-founder of Wikipedia and its second generation version, Everipedia, which is the first ever encyclopaedia to be built on the blockchain.

Aside from a Global Leaders Exchange programme, the two-day summit also opened its doors to the public with a free experiential exhibition that showcased pilot projects and innovative advancements from more than 60 public and private enterprises.

The extensive levels of topics addressed at the Summit included:

- Smart cities, blockchain and regulation
- The paperless race, happiness and blockchain applications
- Artificial intelligence and blockchain
- Start-ups, investor pools and Initial Coin Offerings (ICOs)
- Trust and the blockchain economy
- Integrating blockchain into the private sector

Blockchain technology is an innovative and powerful tool that is already shaping the future through vast, secure and simple transactions.

The Dubai Blockchain Strategy, launched in 2016, and conferences like the Future Blockchain Summit are helping to drive the aspiration of Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, to make it the model metropolis of the future.

The Strategy is built on the three strategic pillars of government efficiency, industry creation and international leadership. As the first city powered by blockchain, Dubai aspires to be the happiest city on Earth, seamlessly integrating the latest technologies to ensure world-leading competitiveness and customer happiness across all services.

Blockchain will contribute to enhanced productivity and estimated savings of more than AED 11 billion spent annually in Dubai on paper and paper transactions. All government transactions, including visa applications, bill payments and license renewals – over 100 million documents each year – are set to be paperless and transacted digitally using blockchain.

Pioneering science, technology and creativity

Dubai is the global leader in committing to adopt this transformational technology to ultimately improve the lives and happiness of its citizens. Beyond this, Dubai is also acting as a pioneering catalyst and collaboration platform to innovations in blockchain technology and its applications.

The Dubai Blockchain Strategy rests on three main pillars. The first is for 100 percent of our government's services to be delivered via blockchain.

The second pillar is to provide and enable an ecosystem that can empower start-ups. The final pillar is to position Dubai as a global thought leader in blockchain. It is important to stress that technology development is not viewed as an end, but as the means to spread happiness.

Innovative economic opportunities

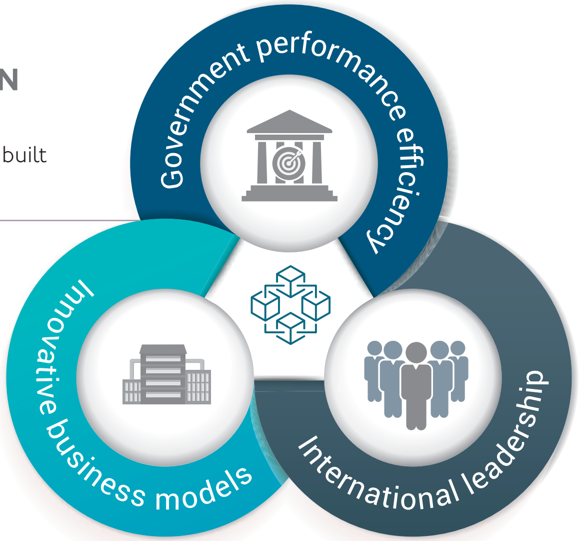
Dubai is world renowned for its 'get-it-done' attitude, with unprecedented progress that has drawn astonishment and admiration over the years.

Now, the city is pioneering the application of leading digital innovations, becoming a global technology leader in the smart economy, and fuelling entrepreneurship and global competitiveness.

Blockchain is already being implemented in most of Dubai's local government departments, including Dubai Electricity and Water Authority (DEWA), the Department of Lands and Property, Dubai Municipality and the Health Authority, to name just a few. Upon successful achievement of its technological strategy, Dubai will cement its leadership position as the first blockchain-powered government.

DUBAI BLOCKCHAIN STRATEGY

Dubai Blockchain Strategy is built on 3 strategic pillars:



HE Yousuf Hamad Al Shaibani: DESC is the reliable security partner of all the government entities in Dubai

HE Yousuf Hamad Al Shaibani, Director General of Dubai Electronic Security Center (DESC), unfolds the Center's strategic role in supporting the vision for Dubai as it proceeds towards a future in which it is the world's safest city in cyberspace: "Our role is to raise awareness among community members about the risks of internet fraud and to increase their knowledge about cybersecurity and everything related to using the internet."

Al Shaibani: "With the aim of securing Dubai's cyberspace to make it the safest city electronically, DESC is perpetually working to implement the Dubai Cyber Security Strategy that was launched by His Highness Sheikh Mohammed bin Rashid Al Maktoum in 2017. DESC's main priority is to protect and support Dubai in this vision by securing it against cyberspace risks and threats. Our key objective is to provide individuals and institutions in Dubai with safe access to the internet, protect their privacy and data, and secure and safeguard Dubai's digital wealth."

"Our role is to raise awareness among community members about the risks of internet fraud and to increase their knowledge about cybersecurity and everything related to using the internet, whether it's simply to browse, to access government or banking services, or even to shop or communicate with others. As Dubai is advancing towards digital transformation, we aim to create a flourishing society that is highly aware of the cyberspace risks and able to stay vigilant against cyberattacks."

"In addition to our awareness-raising initiatives, our tasks include developing and implementing information security policies for Dubai government, combating all forms of cybercrime and IT crimes, supervising the implementation of the criteria set to ensure cybersecurity, and providing technical and advisory support to all government entities. We are the entrusted cybersecurity guardian of all government entities in Dubai. Cybersecurity can no longer be disregarded; in fact, it's at the heart of all tasks and services."

Al Shaibani stressed on the importance of awareness, saying: "A major part of our role consists of raising awareness about cybersecurity threats and risks and encouraging individuals, companies and government institutions to take the necessary protection measures. We develop programmes and various communications, by organizing workshops and orientation sessions designed to urge people to take the necessary safety measures, including protection against malware, and setting strong passwords for e-services portals and smart devices. We also encourage users to employ appropriate firewall and network security tools, install system updates regularly, use social media platforms cautiously, and ensure the security of a privately owned Wi-Fi network."

Al Shaibani also stressed the importance of implementing the relevant criteria for government institutions and private companies in Dubai. "We are responsible for guiding government institutions to take the necessary measures against cybersecurity threats. At DESC, we developed Information Security Regulations (ISR) that include three objectives: firstly, to implement general mechanisms that help limit and prevent any sensitive information that is susceptible to being exposed due to any security breach, thus maintaining the good reputation of Dubai government entities; secondly, to develop a unified regulatory approach to information security at the level of Dubai Government; and, thirdly, to identify the responsibilities assigned to each entity to maintain sound information security practices."

"We have made this system mandatory for all Dubai government entities. The private sector should also consider implementing information security management standards, such as ISO/IEC 27001. Other standards that can be considered are ISO/IEC 27035 (Information Security Incident Management), ISO/IEC 27031 (ICT readiness for business continuity), ISO 22301 or NCEMA 7000."

"These certificates serve as a key element in supporting Dubai's transformation into becoming one of the safest cities in the world. They function to encrypt messages, data and information transmitted by devices to validate users' identities automatically without any human intervention. The ultimate goal is to safeguard our data wealth by ensuring the highest levels of safety and security, which will contribute to boosting digital transactions," Al Shaibani added.

"DESC has also developed a regulatory framework to promote the security and safety of the Internet of Things (IoT). This system is considered the first of its kind in the world, as, so far, there are no internationally recognised policies that secure the Internet as accurately and in such a detailed manner as the approach adopted by this framework. It consists of a number of basic rules that should be referred to as a reference when IoT systems and applications are used by any government or semi-government entity."

> Our strategic goal is to transform Dubai into a secure cyberspace, reinforcing it by spreading awareness and the culture of security among its people and institutions
>
> **Yousuf Al Shaibani**

"We adopt cutting-edge technology in designing and developing cybersecurity solutions to meet the increasing demands of the tremendous development that is being achieved in the digital world. Cybersecurity has become a strategic pillar for the sustainability of life as well as the work of government and private sectors. Therefore, DESC is keen to develop and hone the capabilities and skills of UAE nationals in the field of cybersecurity. The Center has recently established partnerships with several academic institutions with the aim to develop scientific disciplines that will be in demand by the cybersecurity industry in the near future," Al Shaibani explained.

DESC introduces new cybersecurity licenses to boost confidence and growth

In establishing Dubai as a global leader in innovation, safety and security, the Dubai Electronic Security Center (DESC) employs the city's bright young minds and their innovative ideas. Ayesha Mohammad, Permits Officer, is one such dynamic young professional, assigned to develop DESC's licensing activities in collaboration with the Dubai Department of Economic Development (DED). Esharat interviewed her about the new initiative of trade licenses for cybersecurity-related companies.

Ayesha was a fresh Business Administration graduate of the Higher Colleges of Technology in Dubai when she joined DESC in 2017 to develop this new regulatory initiative.

"Groundwork for the cybersecurity sector regulation began in January 2017. Everything that we do at DESC must have a strong motivation and a solid foundation so upon initiating a new project we research the market thoroughly, examining aspects like the primary needs, resources, sustainability, and impact on the future. For me, putting theory into practice and diving straight into the field is the best learning experience," she said.

Benchmarks and objectives

DESC's main mission is to protect Dubai by overseeing the cyber activities that attract international investors, making it a leading hub for technologies and applications of the future.

"We gathered numerous sources to draw up a blueprint that would be ideal for this region. Ultimately, there are four objectives that will be achieved through the implementation of these licenses: Firstly, in line with the DESC mandate, they address the increasing prevalence of cyber threats and the need for expert cyber advice. They also ensure that the cybersecurity services provided in Dubai follow international standards and reassure the business sector that cybersecurity service providers are verified by DESC. In the greater scheme of things, the certified support of DESC will also facilitate the growth of the cybersecurity services market and encourage innovation."

Collaboration not coercion

"Even businesses promising to deliver sophisticated protection from cyberattacks could, in fact, be a source of cyber danger – whether intentionally or simply because they are not as fully qualified as they claim to be," Ayesha explained.

"By June 2017, we were ready to test the waters and tentatively placed the new service on DED's licensing portal. DED was the logical place from which to introduce the cybersecurity business regulation, because they are the first government stop in the establishment of any new company. This is where a business must register its activities before opening its doors."

"Within the first few months, without any marketing to support or drive the initiative, 18 companies added one or more of our cybersecurity activities to their permits!

> The certified support of DESC will facilitate the growth of the cybersecurity services market and encourage innovation

Leading cybersecurity companies operate in Dubai

> Our vision at DESC is to encourage businesses and not coerce them or hinder their operations

This enthusiastic response confirmed that there is indeed awareness and interest for official support in the industry."

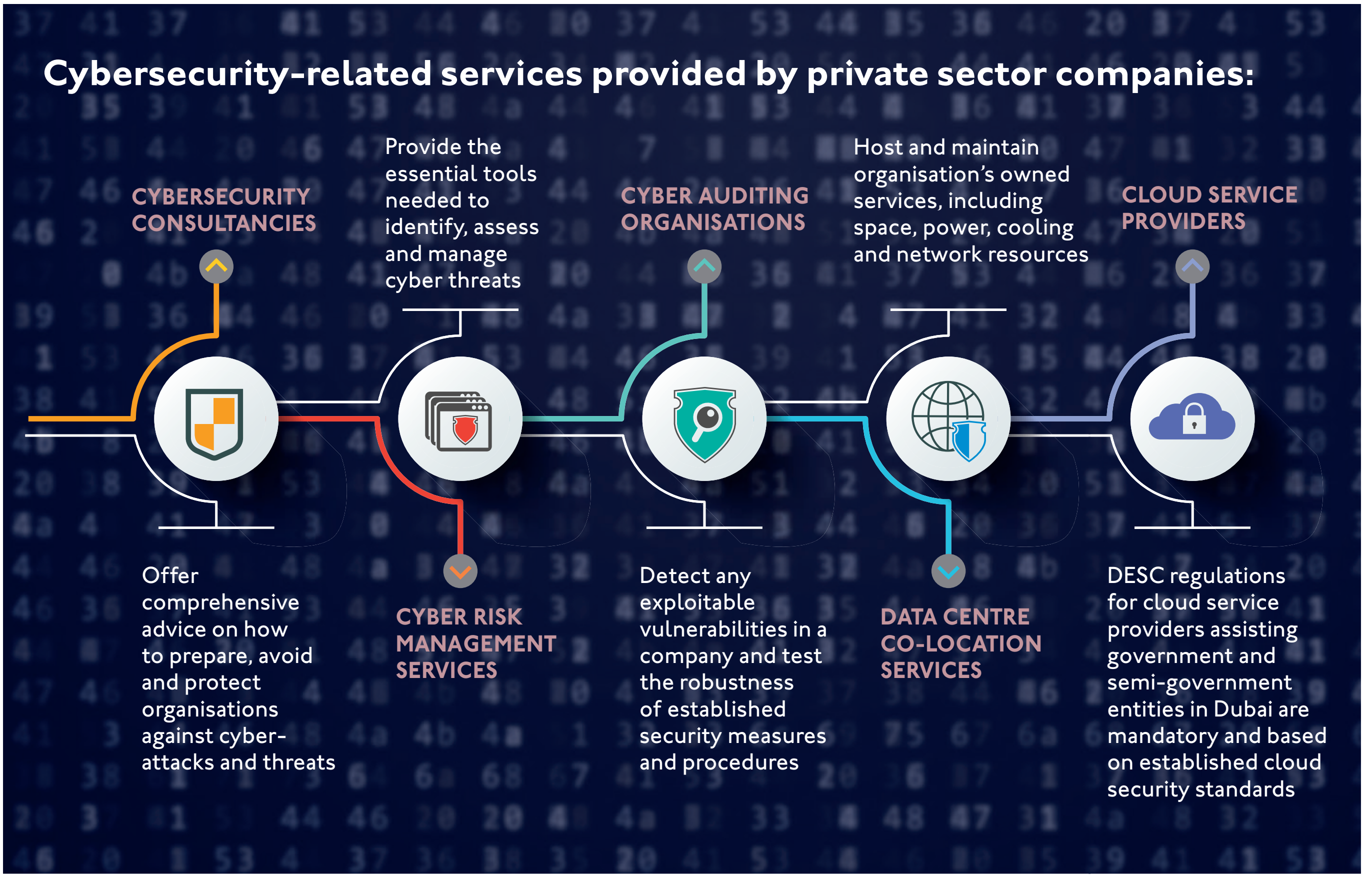
"Although DESC is a regulatory body, our vision is to encourage businesses and not coerce them or hinder their operations. We want to make them aware of the advantages of such a system. The process is still open to final developments and it is important that its introduction is smooth and beneficial for companies."

"Cyberthreats can come from anywhere, at any time. Cybercriminals are opportunistic, so the race is on to make sure they don't leap too many steps ahead. Organisations need to know where the threats are likely to come from and how to prevent them or stop them in their tracks. It's really a job for cybersecurity specialists," Ayesha explained.

The UAE is among the most targeted countries for cyberattacks in the Middle East and Africa (according to Kaspersky Security Network's real-time cyberthreats map).

What types of cyber businesses should be licensed by DESC?

The new regulations verify and support the work of all organisations offering cybersecurity-related services. These include:



Cybersecurity-related services provided by private sector companies:

CYBERSECURITY CONSULTANCIES

Offer comprehensive advice on how to prepare, avoid and protect organisations against cyber-attacks and threats

CYBER RISK MANAGEMENT SERVICES

Provide the essential tools needed to identify, assess and manage cyber threats

CYBER AUDITING ORGANISATIONS

Detect any exploitable vulnerabilities in a company and test the robustness of established security measures and procedures

DATA CENTRE CO-LOCATION SERVICES

Host and maintain organisation's owned services, including space, power, cooling and network resources

CLOUD SERVICE PROVIDERS

DESC regulations for cloud service providers assisting government and semi-government entities in Dubai are mandatory and based on established cloud security standards

- Cybersecurity consultancies
- Cyber risk management services
- Cyber auditing organisations
- Data centre co-location services
- Cloud service providers.

"These types of businesses are relatively new to the marketplace, as their services have only really come into play with the technological developments of the fourth industrial revolution. As DESC, our task is to provide Dubai's government and business sector customers with the confidence that the expertise of their cybersecurity service provider is of an excellent international standard."

"These licenses will also support the reputations of businesses and contribute to their success – so this licensing initiative benefits both customers, who have peace-of-mind knowing they are using a company they can trust, and the service provider, whose skills and integrity are backed by a regulating authority."

DESC's licensing requirements include checking that a cybersecurity organisation and its personnel hold the appropriate qualifications, professional competencies and industry certifications. These vary, depending on the area of expertise.

Supporting this fast-growing sector

"There are already dozens of cybersecurity-service companies registered in Dubai and the market is growing at a rate of 8 to 12 new cybersecurity trade activities per month. DESC has jointly hosted two informative workshops with DED so far. These were attended by over 30 companies, who were extremely responsive to the initiative and some even registered for the license the following day."

"It's rewarding to know that our projects will have such a positive impact on the future well-being of the city, both on the streets and in cyberspace. DESC places great emphasis on the value of collaboration. By using our expertise and guiding principles, we can establish partnerships with public and private sectors that will, indeed, make Dubai the safest city in the world from an electronic perspective."

Further information regarding the DESC license for cybersecurity services can be found on the DED website: www.dubaided.ae

> The authoritative government stamp of approval will support the reputations of businesses and contribute to their success

New cybersecurity standard for autonomous vehicles

Dubai Electronic Security Center has shifted into higher gear on the road to 2030, recently launching a pioneering 'Cyber Security Standard' for the autonomous vehicles that will soon become a regular feature on our bustling city streets.

The Standard is a milestone on the journey of excellence of the Dubai Cyber Security Strategy, initiated under the direction of HH Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, which aims to ensure a safe and secure cyberspace for the city.

At the technological forefront

HE Yousuf Al Shaibanai, Director General of DESC said, "Dubai is considered one of the forefront modern examples of evolving and developing cities and we have great appreciation for the aspirations of the wise leadership that have advanced us to utilize disrupting technology such as self-driven cars."

"DESC works diligently along with its government partners to establish the best practices and standards, the adoption of which will enable and secure these emerging technologies against any challenge. Attaining a high level of security with the introduction of autonomous vehicles will ensure a smooth move into an era where human drivers are not needed and where self-driving vehicles can be fully trusted to transport people in city traffic or on long trips, safely and without disruption."

The development of the autonomous vehicles standard draws upon the Dubai Autonomous Transportation Strategy, which aims to transform 25% of the local transportation in Dubai to autonomous mode by 2030. The strategy estimates that AED22 billion will be generated in annual economic revenues by effectively reducing transportation costs, environmental pollution and traffic accidents.

Dr Bushra Al Blooshi, Head of Research and Innovation, DESC.

Dr Bushra Al Blooshi, DESC Research and Innovation Director, explained that the initial phase structure of the Cyber Security Standard was developed by conducting a survey and analysis of the scope of cyber threats and potential risks facing autonomous vehicles. She said the Standard "extensively covers aspects such as the vehicle's communication security, software security, hardware security and supply chain security."

The Cyber Security Standard will provide the requirements and guidelines for all autonomous vehicles and will be used by the relevant Dubai government departments to aid them in securing the revolutionary forms of transportation.

Benchmark security

An autonomous vehicle is termed a cyber-physical system – meaning that it combines elements of both the physical and virtual worlds. This makes it vulnerable to potential threats involving not only traditional cyber attacks against the information and running of the vehicle, but also a new breed of criminal activity such as remote hijacking and ransomware.

The networks that connect autonomous vehicles – from traffic control features to the financial systems that process payments – also need to be secured.

Dubai aims to be at the cutting edge of mobility so as to ensure that residents and visitors can get where they need to be – safely, efficiently and happily. In addition to driverless vehicles, technologies like smart traffic lights, smart parking and smart tolls all reduce stress on the transportation infrastructure and assist the fast, fluid city flow.

The work of DESC is contributing substantially to robust, fool-proof and criminal-proof cybersecurity for driverless cars, and the systems and infrastructure required to ensure the successful rollout of connected and automated vehicle technology.

Dubai's Autonomous Transportation Strategy Aims for 2030

18 billion increase in public transport efficiency ratio (20%)

396 million increase in individual productivity hours (13%)

900 million reduction in transportation cost per km (44%)

1.5 billion reduction in environmental pollution (12%)

DESC launches Cyber Intelligence Research Lab at the University of Dubai

Dubai Electronic Security Center (DESC) has launched a first-of-its-kind laboratory in the MENA region to create unprecedented research innovations designed to face future cybersecurity challenges. The lab, which is funded by DESC, was established at College of Engineering & Information Technology (CEIT) at University of Dubai.

Inaugurated by HE Yousuf Hamad Al Shaibani, Director General of Dubai Electronic Security Center, and HE Dr Essa Al Bastaki, President of the University of Dubai, the lab is specialised in unconventional cybersecurity research. It keeps pace with the global developments in the fields of artificial intelligence, data revolution and the Internet of Things (IoT). These scientific studies will help DESC develop cybersecurity solutions to protect Dubai's digital wealth on an ongoing basis, enabling the Center to anticipate digital challenges and threats before they occur.

Commenting on the announcement, HE Yousuf Hamad Al Shaibani said, "The vision of our leadership is not limited to planning and preparing for the near future, it also places emphasis on developing strategic plans and solutions that meet the needs of Dubai and support its position as a leading global city for decades to come. With this novel lab, we look forward to contributing to building a generation of national cybersecurity experts who are capable of working on innovative projects that address real challenges, in collaboration with various government and private entities in Dubai."

For his part, HE Dr Essa Al Bastaki said, "The University of Dubai seeks to achieve the UAE Vision 2021 by promoting applied scientific research that serves the institutions supporting this vision." He also stressed the importance of the cybersecurity research lab in protecting society from hostile cyberattacks and hacking.

DESC launches a platform to ensure government compliance with cybersecurity indicators as part of Government Excellence System

Dubai Electronic Security Center (DESC) has launched a platform to support the compliance of government entities with the cybersecurity indicators that must be implemented as part of the Dubai Government Excellence System of the Dubai Government Excellence Program (DGEP) of the General Secretariat of the Executive Council of Dubai.

DESC announced the platform during a workshop organised to raise awareness among Dubai government entities of the cybersecurity indicators' requirements. Thirteen cybersecurity performance indicators were included within the criteria of the Leading Government Entity category, which is based on the five key pillars of the Dubai Cyber Security Strategy.

HE Yousuf Hamad Al Shaibani, Director General of DESC, said, "Achieving the vision of the leadership to make Dubai the safest electronic city in the world requires joint forces, follow-up and implementation of the best standards in cybersecurity. This is what we seek to fulfil through the sustained cooperation with our government partners."

For his part, Hazza Khalfan Al Nuaimi, Acting General Coordinator of the Dubai Government Excellence Program, stressed the importance of Dubai government compliance with the cybersecurity criteria. "We are confident that the government entities will implement these standards and indicators to assert its global leadership and achieve the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai," he said.

DESC and UoS launch the first Internet of Things security testbed in the UAE

Dubai Electronic Security Center (DESC), in partnership with the University of Sharjah (UoS), launched the UAE's first Internet of Things (IoT) security testbed, which allows various organisations to verify the effectiveness of existing cybersecurity measures on their IoT-enabled devices.

The Center explained that the testbed is a research-based interactive platform specialised in analysing data, identifying vulnerabilities, and detecting security breaches in commercial IoT devices.

Present at the event was Dr Bushra Al Blooshi, Director of Research and Innovation at DESC, who said, "We are proud of our partnership with the UoS. Through the Dubai Cybersecurity Strategy, we aim to develop and implement cybersecurity practices that will secure the digital transformation of Dubai into the safest electronic city in the world. The launch of the IoT security testbed today is a constructive step in that direction."

Prof Al Merabti, Dean of College Sciences at UoS said: "We are honoured to partner with DESC on this breakthrough project. The launch of the IoT security testbed is an initiative dedicated to serve the UAE and meets its aspirations to become the best globally. It is a great opportunity for students to get job placements based on their competencies, knowledge and experience as cybersecurity professionals."

DESC hosts seminar on future cybersecurity with IEEE

Dubai Electronic Security Center (DESC) organised a seminar entitled "Cyber Intelligence Summit" in collaboration with the Institute of Electrical and Electronics Engineers (IEEE), UAE Section, to raise awareness about the latest technology in cybersecurity, in line with Dubai's strategy for safe digital transformation.

The seminar was attended by cybersecurity experts and researchers from government entities, the private sector, research centres and universities in the UAE. The speakers shed light on the global challenges of cybersecurity as well as innovative solutions to overcome the rising and ever-changing threats.

Dr Marwan Al Zarouni, Director of the Information Services Department of DESC, said, "On our digitalisation journey, we look forward to placing Dubai among the world's most secure cities electronically, while creating world-class digital experiences that aim to employ the latest technological developments and build a more secure society that is perfectly aware of cybersecurity threats."

Cyberspace Leaders

An initiative for school students to educate them about cybersecurity through risk prevention

As part of its commitment to increase community awareness about cybersecurity, Dubai Electronic Security Center (DESC) organised the "Cyberspace Leaders" programme for school students aged between 14 and 18 years.

Launched under the theme #Awareness_is_Security, the programme was implemented and supervised by experts in the field of electronic security, in cooperation with ICDL, and continued until 7th August. Students were introduced to a set of principles related to digital security, including the safest use of the internet, applications and smart devices.

Hassan Abdulla, Director of Support Services at DESC said: "Educating our students about cybersecurity risks and encouraging them to use their information technology safely is one of the key defence lines against digital attacks and hacking attempts. It's a well-known fact that the majority of attacks happen because of the lack of cybersecurity awareness among community members. The camp focused on this age group to raise their awareness and hone their cybersecurity skills so that they may serve as ambassadors for awareness and digital security in society. We have covered the most important skills and concepts that will enhance their ability to identify and prevent digital attacks before they occur."

UAE pushes the boundaries of technological innovation

The United Arab Emirates government is placing transformative technologies, like deep learning, machine learning and artificial intelligence, at the forefront of its strategic plans for the future.

Already, the bold and futuristic vision of the country's leadership has established the UAE as a world leader. Its UAE 2031 Artificial Intelligence (AI) Strategy, launched in 2017, aims to speed up government's performance and create a highly productive environment that is conducive to the creativity and innovation so critical for progress and success.

Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, has emphasised that AI technologies will drive development in the next decade. The AI Strategy is the first major project in the UAE's far-reaching Centennial 2071 plan. Sheikh Mohammed has called on Emiratis to specialise in the field of AI "to serve our supreme national interests" as the implementation of AI technologies will help develop new sectors and create opportunities for the local economy.

The first of its kind in the region, the AI Strategy covers nine vital government sectors and services. Among its five critical themes is the development of capabilities and skills for higher governmental leaders and officials through training courses and awareness programmes. The world's first ever Minister of State for Artificial Intelligence was announced in the UAE in 2017, and an AI leadership work team, the UAE AI Consultative Council, was formed in March 2018 to oversee the development, implementation and safe use of AI.

Ultimately, these technologies are seen not simply as intriguing futuristic developments but as highly effective tools that can accelerate the governments objectives, improve quality of life for its citizens and residents, and ensure that the UAE is one of the world's best countries by 2071.

The AI Strategy's KPIs for 2031 include a 30% boost in GDP, 50% reduction in annual government costs, 90% resistance to financial crises, and 100% use of AI in government services and data analytics.

Adding real value

Thus far, government has implemented 26 mechanisms to promote the development of AI in numerous economic sectors, both public and private. Some of the great benefits of AI include the streamlining of all operations within a smart city, such as Dubai. Infrastructure systems – from traffic flow and power consumption to public safety and more – can be optimised to maximise efficiency and reduce government costs.

In the public sector, construction and manufacturing are expected to reap the most significant rewards from AI, while retail, health and education will also gain. Research centres, such as the AI Lab, have been established and various related academic programmes introduced in the UAE's schools and universities, to develop appropriate AI skills pools and prepare future generations for anticipated job opportunities. A Bachelor's Degree in Artificial Intelligence is now available in Dubai, for example, in which AI-related science subjects, including coding and implementation, are studied.

Joining global leadership

According to research, conducted by respected multinational financial services giant PwC Middle East, disruptive technologies implemented by the government, like AI, will contribute an estimated AED353 billion to the economy by 2030, boosting the UAE's GDP by almost 14%. The global economy is expected to gain as much as AED57.8 trillion from AI by then, but, even before then, the country's refined strategies, efficiencies and future opportunities will position the UAE to compete on par with international elites.

The PwC Middle East report noted that the UAE government's strategic "initiatives to support the development of AI places it in a strong position as one of the leaders for AI in the region and, quite possibly, the world. For example, Dubai's strategies include, amongst others, a Smart Dubai Strategy, a Dubai 3D Printing Strategy, and a Dubai Autonomous Transportation Strategy".

Making Dubai safer and happier

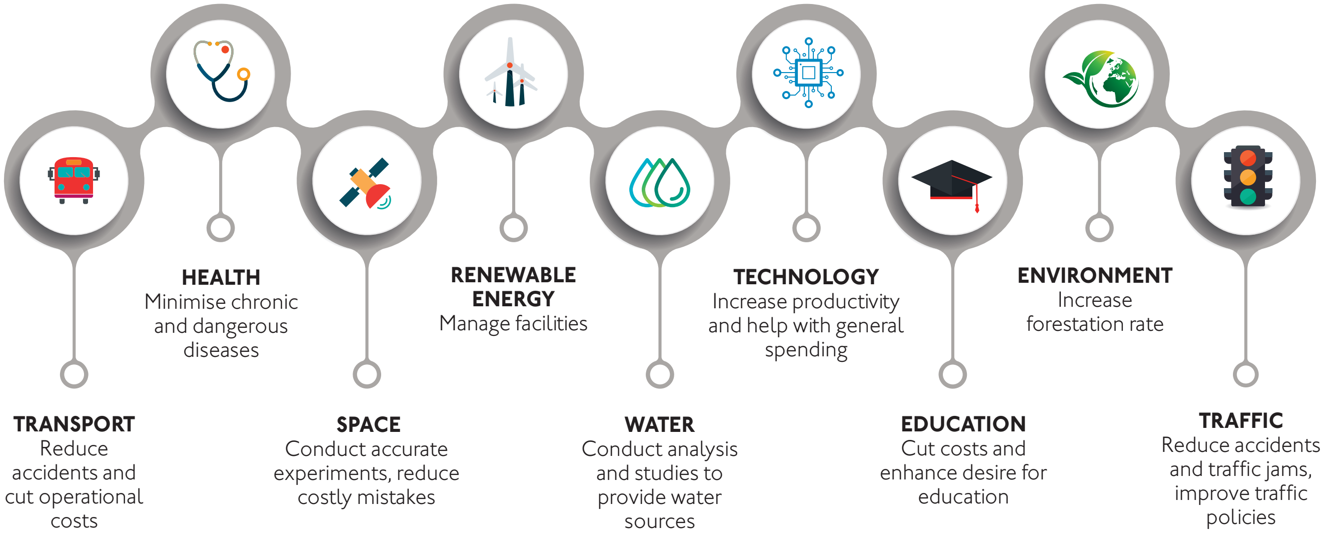
Cybersecurity technologies that involve deep learning, such as machine learning and artificial intelligence (AI), are on the rise. When these machines are provided with data related to potential security threats, they are able to make independent decisions to block any potential breach to the information system.

Did you know that Dubai has the world's first artificially intelligent robot policeman patrolling its streets? It officially joined the police force in May 2018 and, by 2030, the robotic team will probably make up one quarter of the entire Dubai squad.

Dubai Autonomous Transportation Strategy is targeting a similar figure, with 25% of vehicles either on the road or in the sky providing driverless transport by 2030. The Dubai Electricity and Water Authority (DEWA) also recently introduced five AI robots at its Customer Happiness Centres, which can handle numerous enquiries simultaneously.

AI's star quality will be showcased at Expo 2020, where Dubai expects to welcome more than 20 million visitors over six months. A host of astonishing AI-powered tools are planned for the event, including customer service, crowd management and smart marketing. AI technology will be used to enhance the visitor experience with shorter, faster queues, personalised and responsive information through mobile apps and chatbots, and heightened security that can recognise faces and recall visitor profile data.

UAE Artificial Intelligence Strategy focuses on these sectors:



TRANSPORT
Reduce accidents and cut operational costs

HEALTH
Minimise chronic and dangerous diseases

SPACE
Conduct accurate experiments, reduce costly mistakes

RENEWABLE ENERGY
Manage facilities

WATER
Conduct analysis and studies to provide water sources

TECHNOLOGY
Increase productivity and help with general spending

EDUCATION
Cut costs and enhance desire for education

ENVIRONMENT
Increase forestation rate

TRAFFIC
Reduce accidents and traffic jams, improve traffic policies

Online shopping - look after yourself out there!

Online shopping is surely one of the most fun, convenient and time-saving innovations to have emerged out of this exciting and increasingly virtual new world! You can send your grandmother flowers, research the best deals on that hot red sportscar you've been eyeing, grab a pair of cool sunglasses while they're on sale, or do the boring grocery shop... all from the comfort of your couch!

Before you punch in your credit card details, though, it's really important that you've buckled in some basic online safety precautions.

Technology has certainly made great strides in security over the years. But you should be aware that every time you make an online payment there is a slight risk that someone with bad intentions will try to get their hands on your personal and financial information or trick you into paying for something you will never actually receive.

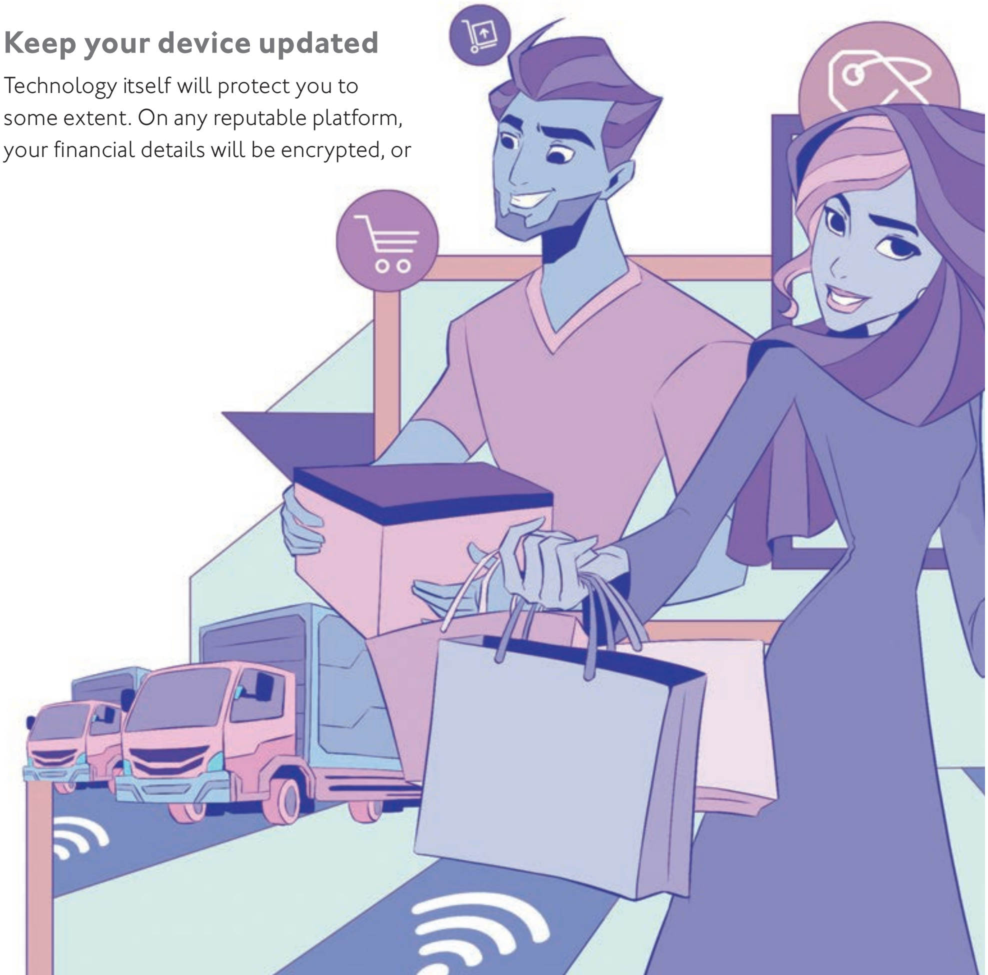
You can protect yourself and enjoy peace-of-mind online shopping experiences. Here are some top tips from the experts:

Keep your device updated

Technology itself will protect you to some extent. On any reputable platform, your financial details will be encrypted, or converted into a code that is impossible to read. But you do have to keep your operating systems and third-party apps up to date! It may seem a bit of a hassle, but updates are armed with important changes – including those that take care of the latest security flaws – that will ensure your software continues to run safely and efficiently.

Practice safe tech

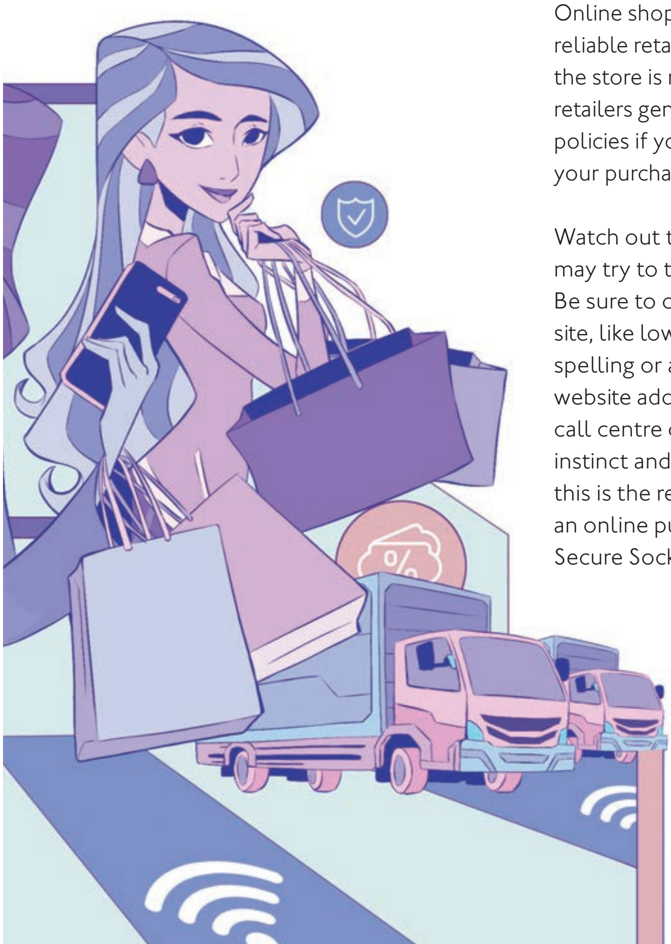
Practice good digital hygiene by not visiting dodgy websites or clicking on suspicious ads and never open an email attachment from an address you don't trust. And always use a PIN or password to access your smartphone or computer, in case they (physically) get into the wrong hands. Spyware, like a simple keystroke logger that can be spread by malware or loaded while you're not with your device, could provide thieves with your password or banking information.



Select a safe payment method

You can further reduce your risk by choosing the best payment method from the list offered at the online check-out till: credit card, prepaid credit card, debit card or a well-known and trusted third party payment service.

Credit cards are usually well protected against fraud, and there's a good chance you can get any unwanted charges reversed if necessary. Plus, there's that three-digit security feature (CCV code) on the back of the card that provides extra protection. Third party services mean you don't have to share your financial secrets with different retailers – just the one respectable payment provider. Debit cards are usually the cheapest option, but your money does go out of your account straight away. In all instances, be suspicious if you are being asked for more information than necessary. No retailer should need your Emirates ID number! If you are concerned, act quickly and report any unauthorised activity to your bank as soon as you notice it.



Don't be plain with your passwords

Expert hackers claim they can hack even the least likely passwords in a maximum of five attempts – usually sooner! Yes, they are a pain to remember, but it really is safest to have separate passwords for every account, including your computer and phone. Avoid choosing common words or obvious numbers like your birthdate. Mix up letters, numbers, cases and icons. If that's too tricky to remember, try creating a string of words that is actually a short, meaningful sentence, such as: #Digger$loveshisredball.

Stick to the tried and trusted

Online shopping is safest at well known, reliable retailers. This way you can be sure the store is not a scam – plus, established retailers generally have efficient returns policies if you're not entirely happy with your purchase when it arrives.

Watch out though… some clever crooks may try to trick you with a fake website! Be sure to check for tell-tale signs on the site, like low-resolution images, incorrect spelling or a .net instead of a .com in the website address (url). Is there a customer call centre or helpline number? Trust your instinct and call it to make 100% sure that this is the real deal. And only ever make an online purchase on a website that has Secure Sockets Layer (SSL) encryption. In the browser, it will say 'Secure', and there will be a little closed padlock or a key, followed by https:// at the beginning of the url.

Get all the details

Don't just punch in your card number and hope for the best. When making an online payment, take a screenshot or print all the details of your purchase (including a receipt or order confirmation number) so that you have a reminder and proof of your transaction.

Keep your device updated
Practice safe tech
Select a safe payment method
Don't be plain with your passwords
****_
Stick to the tried and trusted
Get all the details

Social media is no place for bullies

INSULTS AND EMOTIONAL ABUSE ARE NOT ONLY UNKIND – THEY MAY BE CRIMINAL!

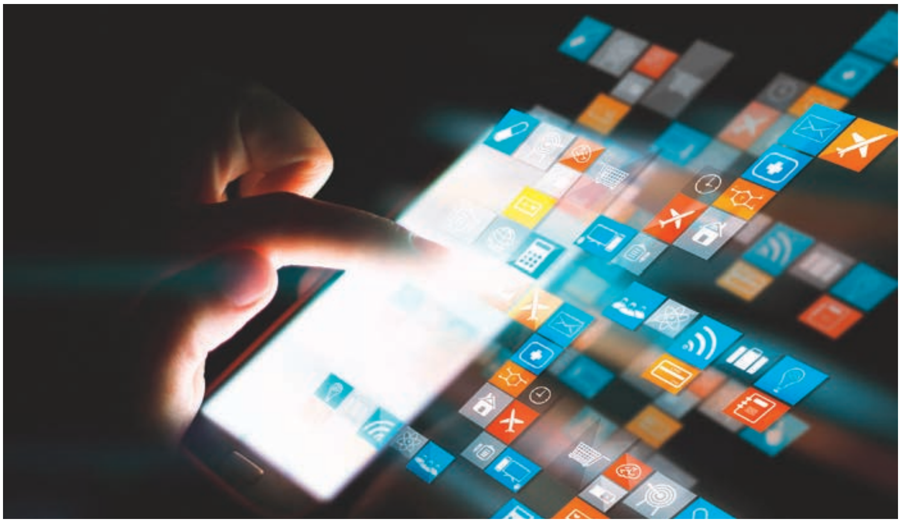
The law in the UAE regards online abuse as an extremely serious offence, punishable with the most severe penalties ranging from financial fines to imprisonment and even deportation.

In recent years, several online abuse lawsuits have been filed, including a case in which the offender was fined AED3,000 for insulting someone on Instagram, another similar abuse case involving WhatsApp, and even one in which a social media celebrity landed himself in jail for posting a video on his Instagram account in which he lashed out with insults and slander.

Esharat interviewed prominent lawyer and legal consultant Youssef Al Bahar to gain insight into these issues. The laws surrounding abuse over social media, he explained, are firm and clear: "Ignorance of the law excuses no one and does not provide relief from punishment. Insulting people and cursing on social networks are offences punishable by law."

Al Bahar said the mechanism for prosecution is simple too. "Any victim who has been subjected to abuse on social media is entitled to contact the relevant authorities to file a report on the incident. He or she must provide evidence of the injustice, such as a screenshot of the alleged abuse and documents to prove that the account belongs to the offender."

Youssef Al Bahar, Lawyer and Legal Consultant



> It is not lawful to file an online abuse lawsuit more than three months after the victim became aware of the crime

Filing a report

"There are many ways to file such a complaint. The victim can lodge a report at their nearest police station, report the abuse through mobile applications or submit their report directly to the Public Prosecutor's office, which will process the legal action and bring the criminal proceedings before the court. However, the case may be dismissed if the court rules lack of evidence or insufficient elements to support a criminal ruling," Al Bahar added.

Penalties

Article 20 of Decree No. 5 of 2012 on Combating Cybercrimes stipulates that "without prejudice to the provisions of the offence of libel stated in the Islamic Sharia, a penalty of imprisonment and a fine of not less than AED250,000 and no more than AED500,000, or one of these two penalties, will be enforced on any person who abuses others or was assigned an act that would make him liable to punishment or disrespected by others, using a website or a smart device".

Al Bahar explained: "The Federal Supreme Court stresses the inadmissibility of any cyber abuse-related claims after more than three months from the day the victims were informed of the crime and its perpetrator, on the grounds that their carelessness about submitting the complaint deprives them from their right in accordance with the Federal Law of Criminal Procedures."

"If the Public Prosecutor decides to refer the case to the Criminal Court, it will be presented at different stages of litigation. If the court finds that the defendant is guilty, the victim gains the right to appeal to the civil court to claim compensation."

Understanding the abuser

Social media users should be cautious when saying or writing anything abusive or they may find themselves accountable and facing severe consequences. It is best for victims to avoid aggressive, angry responses when provoked so as not to give the abuser any chance to continue their insults and antagonism.

The abusive personality can be described as hostile - such an individual may express offensive words to compensate for a lack of self-esteem and to achieve a sense of victory. On the one hand, the abuser may be ignorant of the legal culture surrounding insults and defamation; however, some social media users actually provoke others in order to incite them to engage in forbidden hate speech, thereby involving them in criminal cases that may include fines and imprisonment. This is another reason why social media users should not rush into posting offensive words and should think carefully before reacting to insults. In fact, it is wise to simply ignore bullying behaviour altogether.

Social media etiquette

Social media users should not allow others to provoke or annoy them, and should be as tolerant as possible towards the diversity in online communities. It is best to ignore abusers and always maintain a decent behaviour and attitude.

All on social media should avoid spreading rumours and false news. It is always best to double check that news is true before it is posted.

Unfortunately, there are people who like to use social media to defame and press false charges against others. They often resort to such behaviour as a means of venting against the pressures of life, using words that are contrary to decent public morals. Many social media users hide their true identities by assuming fake personalities and wearing a different mask for every occasion. Sometimes, they will even assert themselves as moral guides or critics and use offensive words, slander and insults that they never would in real-life situations. Others may spread lies and rumours that affect one group of people and provokes them to insult another group. They exploit public events, such as the World Cup, which became a platform for fierce social network battles and abuses among online fans.

It is important to always be tolerant of others, especially those we know only through the small screen, and to choose trustworthy accounts so we can communicate in a safe and reliable way.

> It is wise to simply ignore bullying behaviour altogether

> Social media users should behave wisely and not allow others to provoke or annoy them; they also need to be as tolerant as possible towards online communities

Counting the cost of cybercrime

There's no doubt that cybercrime is on the rise… but how much is it really costing the world's economies? The latest statistics, published by McAfee and the Centre for Strategic and International Studies (CSIS), put the figure at well over AED2,000 billion, or approximately 0.8% of global GDP. Shocked? Read on…

The relentless growth in cybercriminal activity sheds startling clarity on the importance of ensuring the cybersecurity of Dubai. Esharat looks at some of the most astounding data from the report:

- The statistics show massive growth from the 2014 figure of $445 billion.
- In terms of crimes with global economic impact, cybercrime now ranks third, after government corruption and narcotics.
- The costs of cybercrime include the results of malicious attacks to personal, business, organisational and intellectual property, as well as damaged reputations and lost opportunities.
- The lower cost of entry and radical advancements in technology, including artificial intelligence, have made it even easier for criminals to infiltrate cyberspace.
- While cybercriminals quickly adopt the latest attack technologies, new internet users are mostly in countries with weak cybersecurity.
- Certain countries have, perhaps unwittingly, become a safe haven for cybercriminals. Records show that the unlawful activities in some places tend to be for financial gain, while in others they are more often linked to espionage.
- The cost of cybercrime varies across regions, depending on the sophistication of different countries and their cybersecurity measures.
- The menace of cybercrime is universal, which is why it is so important for countries to work together to maintain control.

Every day…

80 billion scams are launched

33,000 phishing attacks occur

4,000 ransomware threats are made

780,000 records are lost to hacking

(McAfee and the Centre for Strategic and International Studies)

How safe are your child’s video games?

Some video games and smartphone app games pose a real risk to the safety of their users, not only hacking their privacy and leaking their personal data, but even affecting children’s behaviour and encouraging problematic conduct among teenagers, including violence and aggression.

According to Faisal Al Shammari, CEO of Emirates Society for Child Protection, the popularity of video games has spread widely over the past few years, particularly amongst children and youth. “Some of these games are highly dangerous, posing risks to our children’s lives. We monitored these games and raised many awareness campaigns to boycott them because of their alarming negative effects. They encourage children and teenagers to inflict violence and develop dangerous behaviours that can lure them into committing self-harming practices. Such games can also be an ideal environment for privacy violation and blackmailing by leaking users’ personal information.”

In addition, certain games have a negative impact on social skills as they lead to social isolation, thus reducing children’s inclination to take part in sport and exercise or to socialise with others, both of which are important in promoting communication skills and enhancing the growth of their personalities. Video games addiction has also been clearly linked to mental health problems. However, parents can adopt certain preventive and proactive approaches that can help to reduce the risks imposed by some games, particularly those that include distressing scenes of violence.

Faisal Al Shammari, CEO of Emirates Society for Child Protection

Al Shammari has called for tighter control over the purchase of video games and

promotes the rating of their content according to age appropriate categories. He urged all concerned parties, including family members, school and community institutions, to participate in preventing the spread of dangerous video games.

Imitating violence and negatively challenging the spirit

Dr Huda Al Suwaidi, Director of Family Development Department at the Community Development Authority in Dubai, confirmed that scenes of violence in video games have a significant impact on children's

Huda Al Suwaidi, Director of Family Development, Community Development Authority

Advice to protect children from harmful digital games:

Check the rating

It will provide age suitability, content description & interactive elements.

Activate parental controls

Password-protected settings should include limits like play time and an approved friends list.

Teach healthy habits

Safety rules for real life – like not sharing personal details – also apply in the digital world.

Get involved

Play games with your children. It will help you to stay in touch with their online activity and they'll think you're super cool!

Be sensitive to signs

Take note of signs of anxiety in your child during or after digital play. Trust your parenting instincts.

Some video games incite our children to exercise violence and make them vulnerable to privacy violations and blackmail by leaking their personal information

Faisal Al Shammari

CEO of Emirates Society for Child Protection

behaviour, encouraging them to mimic the scenes in real play. She urges parents to research and guide their children in the selection of movies they watch and games they play.

"In light of technological developments, video games have become a vital part of our children's lives. They spend long hours behind their PC screens without supervision. Unfortunately, these games contain scenes of violence and murder, which negatively challenges the spirit, taking a toll on children's personalities and encourages them to commit criminal acts or drives them toward social isolation. Therefore, parents are required to find useful alternatives that will benefit their children, such as encouraging them to develop their talents, to read and to be more involved in sports activities and brain games," she said.

Double-edged sword

"Video games enjoyed by the new generation of children and youth are predominant in today's world, so it is important that they be invested in a positive manner," said writer and educational advisor Hamsa Younes.

Hamsa Younes, writer and educational advisor

"It's our duty as parents to be lovingly involved in our children's lives, accepting their world and helping them to possess the intellectual and moral tools that guarantee their responsible use of these games, even in our absence. It's essential to keep an eye on our children by watching them closely but without the need to supervise them at all times. Supervision is proof of the lack of confidence between the two parties, so it can make our children resort to all types of tricks and may end up in arguments. Our trustful awareness and sharing of these electronic games will cement our relationships with them and give us the opportunity to protect them from the negative effects of these games."

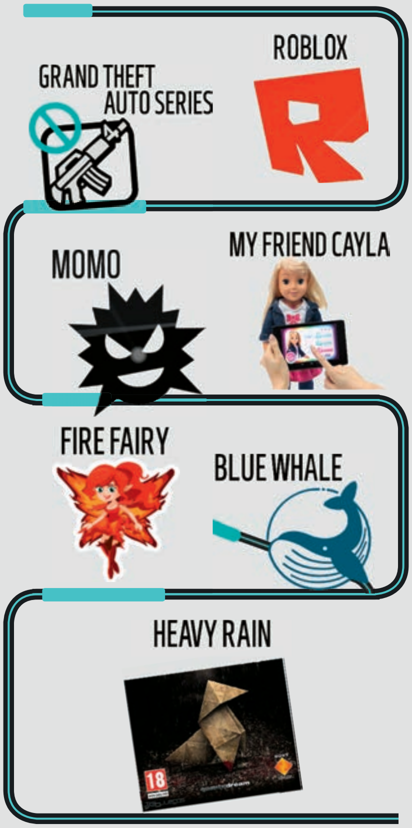
"Most videos games teach children and teenagers concentration skills, eye-hand coordination, planning abilities and problem solving skills. Using these types of games can broaden users' minds and awareness, as the levelling-up patterns in such games actually help brain development, boost the child's self-confidence and stimulate creative thinking, thus developing their ability to suggest creative solutions in various situations," she explained.

However, parents must pay great attention to content and only allow them to play problem-solving games that help them to acquire certain skills and information that enrich their personality and support age appropriate mental development.

"Video games offer great advantages if used properly and for a limited amount of time, set clearly by parents without having to resort to arguments with their children. One of the most dangerous aspects of video games is that the child or teenager gets affected by their scenes of violence to the extent that they become familiar. As a result, the child may inflict violence on parents, teachers and peers, making them socially isolated and vulnerable to stress and anxiety."

"Parents' control over these video games requires them to be actively present with their children. Therefore, we have to demonstrate the harmful uses of these

Some of the best known dangerous and banned video games and smart toys include:



> The UAE law criminalises the violation of privacy in video games
>
> Hamid Darwish
> *Lawyer and legal adviser*

games through dialogue and discussion, while providing appropriate alternatives that satisfy our children's interests," Hamsa added.

Penalties for promotion and privacy violation

To learn how the UAE law deals with issues related to cybercrime offences, including privacy violation, and the penalty for promoting banned video games in the UAE, Esharat consulted lawyer and legal advisor Hamid Darwish, who explained: "The relevant authorities in the UAE have banned the sale and promotion of some video games affecting children's mentality. These games were also prohibited by the National Media Council on the basis that every act that violates morality, honour and public order, or incites video game users to commit a crime or a violation of the law, shall be subject to legal liability."

Hamid Darwish, lawyer and legal advisor

Darwish said that UAE law criminalises the violation of children's privacy in cases of video game crimes under the Cybercrime Law. In addition, the Protection of the Rights of the Child Law states that every child has the right to respect for his or her privacy in accordance with public order and ethics, taking into account the rights and responsibilities of their guardian. It is forbidden to publish, display, circulate, possess or produce any audio-visual publications or games for children that appeal to their base instincts, suggest behaviours contrary to the public order and ethics, or that are likely to encourage delinquency.

What do parents think?

Ultimately, most parents only want the very best for their children and should follow their family values and parental instincts. However, it does help to know how other parents handle difficult issues through their children's different growth phases.

One common consideration is that depriving a child of video games altogether will make him less privileged than his peers. Instead, some parents compromise with a fixed playing schedule that is tied into a reward system. If a child finishes his homework early, for example, he may be rewarded with an hour of supervised video game play.

Even more worrying for many parents in the UAE are those video games that contain obscene scenes inconsistent with the values and traditions of our society. The concerned authorities have been urged to tighten control on these games, deny their access to markets in the UAE and ban them from the Internet and mobile applications.

However, parents also commonly express concern that media-related dangers are not limited to video games, but include cartoon television shows and movies that contain violence. Some younger children get so taken up with the fantasy worlds of their favourite characters, like Spider-Man and Batman, that they begin to imitate them in every respect – even jumping from the tops of high walls or furniture in an attempt to fly like their heroes. There is no question that these young, innocent adventurers need parental guidance and supervision.

Less than 10% of Google users enable their 2-step Gmail security feature

Google has revealed that only a small percentage of Gmail account holders make use of one of its most effective security features: the two-factor verification.

The two-factor authentication (2FA) feature makes it very difficult for any unauthorised person to hack into your Gmail account, even if they manage to get your login details and password.

The 2FA security system can be activated easily by visiting

https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome.

As the name suggests, it involves signing into your account both with something you know (your password) and with something freshly generated and unique (a code sent to your phone). Each verification code can be used only once. It is sent via text, a voice call or Google's mobile app.

Drones vulnerable to cyber attacks

Drones are likely to become a fairly common site in the decades to come. They are quickly being adopted for various purposes, including commercial deliveries. They are useful but, at the same time, invasive and annoying.

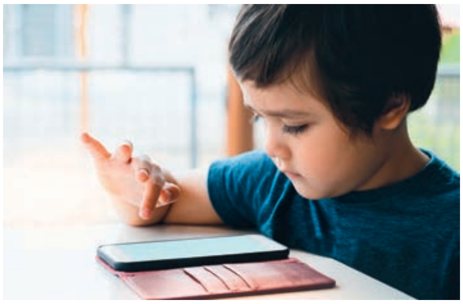
According to Nimo Shkedy, CEO of ApolloShield, who is specialized in systems to detect and block unauthorised drone intrusions, the little unmanned aerial craft are a security nightmare. Those with cameras easily bypass security systems to fly into unauthorised zones, collecting photographic surveillance material that puts people's privacy or safety at risk.

Shooting them out of the air may be unnecessarily hostile and potentially dangerous, so companies are working on a safer and more creative way to get rid of offensive drones, one of which is through digital hacking.

Drones are still a fairly fresh development, not yet equipped with automatic protection from cyberthreats in the way our phones and computer systems are today, and this makes them vulnerable to cyber attacks. Techniques like radio frequency jamming and denial-of-service can force a drone to land before it has accomplished its mission.

Of course, while ethical hacking technology can be used to stop illegal or hostile drone activity, criminal hackers are likely to use the same technology for cyber attacks on drones. This aspect of cybersecurity is predicted to grow into a big industry as drones become a more common sight on our skyline.

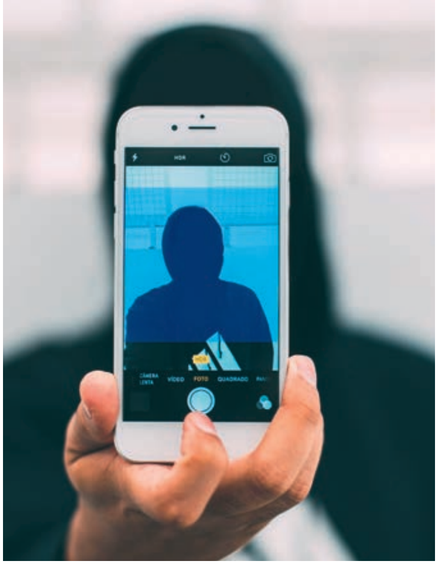
AI algorithms to toddler-proof phones



New software, developed in collaborative research between Chinese and American universities, uses an algorithm to detect when a child is using a mobile device and then automatically block inappropriate channels. This technology could save parents from worrying about their young children accidentally accessing unsafe websites. The artificial intelligence tracks finger movements on a device, using metrics like finger pressure and the length of a swipe. The age-detection software has been 84% accurate in tests with just a single swipe, and 97% accurate after eight swipes.

Facial recognition technology could be a win for hackers

IBM's cybersecurity division has cautioned that our photographs on social media could be used to feed facial recognition technology for malicious purposes.



Our faces are an aspect of online identity theft that most of us do not think to protect as readily as our passwords and pins. But Dr Marc Stoecklin, principal research scientist for cognitive cybersecurity intelligence at IBM, said that if hackers wanted to target a specific person, they could simply harvest their images from social media, infect a computer network and then launch an attack when the target's face was detected. The malware is driven by artificial intelligence and can similarly use indicators like voice recognition and geolocation.

The technology can also be used for good: open source intelligence gathering skills are used to generate leads in missing person cases, for instance. Stoecklin and his team are exploring ways in which AI can best be utilised in cybersecurity by using an open-sourced tool, such as, DeepLocker, to assist white-hat hackers employed to test the security of company networks.

UAE locks in national electronic security with new strategy

The Telecommunications Regulatory Authority (TRA) of the UAE recently launched a national e-security strategy that aims to ensure the country's information and communications sector.

The new strategy is based on five key pillars: preparedness and prevention (to enhance the UAE's cyberspace assets and reduce its risk levels), detection, and response and recovery (which manages any electronic incidents that may occur and reduces their impact).

The strategy will assist the roll-out of national digital security plans, including: ensuring compliance with e-security standards, developing capabilities to manage cyberthreats, and enhancing research and innovation capabilities.

National capacity building plays an essential role in the country's approach to electronic security, as does collaboration. Local and federal bodies coordinate their work, while the strategy also emphasises cooperation between national and international stakeholders to achieve mutual electronic security objectives.

The TRA is responsible for implementing the national framework of the UAE to ensure the security of information, especially at state level, and to entrench standards. Ten major sectors in the UAE fall within the scope of the e-security strategy: telecommunications and information technology, health, water and electricity, emergency services, transportation, the government sector, the financial sector, chemical industries, nuclear power, and the oil and gas sector.

The evolution of the internet:

What will the future bring?

Even the experts can only imagine. Unquestionably, the web itself, developed nearly three decades ago by software engineer Sir Tim Berners-Lee, is also, naturally, evolving. But how? And what kinds of changes on society can we expect it to generate in the future?

Isn't it astonishing how quickly our everyday lives have become inextricably intertwined with the virtual world? The internet is our revolutionary hero, irrevocably and extravagantly altering the evolution of all mankind.

As online social platform Reddit's co-founder, Alexis Ohanian, commented: "To join the industrial revolution, you needed to open a factory; in the internet revolution, you need to open a laptop". For most of the developed and emerging world, that kind of liberty has, indeed, proved revolutionary. And it's all thanks to the foresight and integrity of its creator, Sir Tim Berners-Lee.

As the web began to grow, Berners-Lee realised that its true potential could only be unleashed if anyone, anywhere could use it, totally free of charge and without permission. "You can't propose that something be a universal space and at the same time keep control of it," he explained. The innovative computer engineer ensured that the fundamental internet code would always be freely available to everyone.

Founding principles

Today, Berners-Lee's organisation, the Web Foundation, highlights the principles laid down by the early web community:

Decentralisation – No permission is needed from a central authority to post anything on the web.

Non-discrimination – All users who pay for a certain quality of service should be able to browse and communicate at the same level.

Bottom-up design – Code has been publicly developed and shared to encourage maximum participation, experimentation and usage.

The short, impressive history of the internet:

1958	Computers were properly introduced from the late '50s
1972	First email sent by computer scientist Ray Tomlinson
1982	Word 'internet' first coined
1989	World Wide Web invented by computer scientist Sir Tim Berners-Lee
1991	First website launched by Swiss physics laboratory CERN, where Berners-Lee was working as a software engineer
2007	Launch of the iPhone, delivering the 'internet in your pocket'

And fast forward to...

2019	Today's Fourth Industrial Revolution, incorporating AI, Big Data, the Internet of Things, blockchain, smart so-many-things and seemingly limitless potential for so much more!

Universality – The web requires all computers to speak the same language, no matter the hardware, and no matter the users' geographical, cultural or political differences.

Consensus – Universal operating standards for the web are achieved through a transparent, participatory process at W3C (World Wide Web Consortium), the main international standards organisation for the web.

These principles have guided exciting developments beyond web development, like open data, which promotes and enables unprecedented access to knowledge and information. The empowering effects of the internet on society are far-reaching and have the kinds of positive impact that early creators envisaged: today, a rural shepherd can complete an agricultural degree online, and an up-and-coming poet can publish his creative work and achieve fame without prohibitive printing costs.

> The internet's true potential could only be unleashed if anyone, anywhere, could use it

> Experts are confident that the future internet promises new technologies that can amplify the best of humanity

Slow, steady change for society

It's impossible to know for sure where the evolution of the internet will take us next. Humans being humans, there are those who predict wonders and those who predict gloom, but experts do find common ground with a number of core expectations.

Constant connection – Many of us lived through the early, ear-piercing days of dial-up and are delighted about today's (almost) instant Wi-Fi password connections. One day, internet connectivity will probably be as constant as electricity.

New realms of reality – Augmented reality (such as Microsoft's HoloLens) and virtual reality applications are fast gaining ground, moving beyond gaming to add untold value in fields as diverse as autism and engineering.

Material world integration – Already, there are billions of things connected to the Internet of Things (IoT), from wearable health trackers to automated home energy savers. The IoT makes life easier and cities smarter, and it provides manufacturers with a competitive edge, so it's almost a given that the material things in our lives are going to become increasingly connected.

Cyberworries – In a recent survey of nearly 1500 internet experts, Pew Research Center reported a distinct rise in anxiety related to the future of the web. Respondents raised concerns like interpersonal ethics, surveillance, and crime.

Global communities – Information sharing and connecting through the internet will enhance international connectivity, fostering positive relationships between groups and leading to new, borderless communities.

Open and big data will provide information to help people become more aware of the world and take informed steps to improve it for future generations.

The Internet Society was formed in 1992 by Vint Cerf and Bob Kahn, the inventors of the fundamental communication protocols that underpin the internet. The non-profit organisation works globally to ensure that the internet remains a universally shared resource - open, transparent and collaborative. In-depth research provides society with insight to follow those at the forefront of digital change. The Internet Society website declares its confidence that the future internet "promises social development, economic prosperity and new technologies that can amplify the best of humanity".

While technology will certainly become infused with society in ways that none can yet fully imagine, those in the cyberspace ecosystem are determined that the internet's foundational ideals of open, universal access will never be compromised.

Six simple ways to keep your smartphone safe

It only takes a few minutes to enhance security and privacy on your device.

If you don't consider yourself a VIP (well, not beyond your closest circle anyway), you probably think it unlikely that anyone would want to hack your smartphone. And yet… wouldn't it be awful if your files were encrypted and you lost hundreds of precious photographs? Just imagine if someone accessed your company's emails through your phone and leaked corporate information to business competitors! It happens all the time.

Esharat has sourced the best mobile security tips, making it easy for you to boost the security of your device in a matter of minutes. (You're welcome.)

1. LOCK YOUR PHONE – The screen lock is a basic security tool yet so many people don't use it (usually the same ones who leave their phone lying around). Guilty? Go to SECURITY in your SETTINGS right now and set up a pattern screen lock, password or fingerprint pass (if your phone has this option). Deactivate the option to make the pattern visible and be alert to eagle eyes when punching in your password.

2. USE ONLY SECURE CONNECTIONS – Information sent via public networks is not safe. Never access or handle your sensitive data (like banking codes) using the Wi-Fi in the coffee shop or airport lounge. If there's a transaction you must make or an email you have to send, switch on your mobile data instead. Bluetooth is not a secure means of communication either, so keep it off.

3. CHOOSE SAFE APPS – There's an app for almost everything these days, very nifty, but do resist installing anything you're not 100% sure about. Choose only official app stores apps, do a regular spring clean to uninstall the ones you don't use, and update apps regularly as outdated apps are vulnerable to attacks.

4. BE ALERT FOR PHISHING – Cybercriminals sneak in with such devious tricks that no one is immune to being breached. It's even more difficult to pick up on phishing on your phone than your computer, but the same rules apply. Don't click on any suspicious links and be wary of downloading attachments. Install an ad blocker when web browsing.

5. BACK IT UP – Cloud technology provides us with an alternative safe house for treasured photographs and documents. Should your phone get lost or stolen, at least you won't lose your data. Nearly all operating systems offer the option of automatic backup to a cloud folder, so make sure yours is enabled.

6. REMOTE DEVICE LOCATION – Download the Android option 'Android Device Manager' from Google or the iOS version, appropriately called 'Find my iPhone'. This great dedicated app will make sure you can always track your phone, whether it has been stolen or simply misplaced.

Data security: The cornerstone of the Fourth Industrial Revolution

This is a bold, brave new era for mankind. The 21st century is delivering one jaw-dropping, life-changing innovation after another, from the nanotechnology in 3D printing of human organs, to the smart systems that are helping leading cities like Dubai become seamlessly efficient, secure and strategically geared for a bright future.

At the heart of these astonishing advances is data – the facts, statistics, values and variables about you, me and the entire world, gathered in great swathes of gigabytes, terabytes and petabytes, and then analysed, stored, accessed and utilised in myriad pioneering ways, some noble and others bad.

In fact, the combination of big data and artificial intelligence (AI) is said by many to be the lifeblood of what is increasingly accepted as the world's Fourth Industrial Revolution. Characterised by the incredible fusion between the physical, biological and digital realms, this new era includes developments such as cognitive engineering, quantum computing, robotics, blockchain and the Internet of Things. It's fast, it's thrilling, it's changing the human experience, and it can also seem more than a little scary.

Promises and perils

It was Klaus Schwab, founder and executive chairman of the World Economic Forum (WEF), who first introduced the term 'Fourth Industrial Revolution' in 2016. Schwab cautioned then that "the changes are so profound that, from the perspective of human history, there has never been a time of greater promise or potential peril".

There is no doubt that, along with its progress, the era also brings unprecedented threats. Yes, there is that vague niggling worry about robots taking over the world – honestly, not yet a priority concern for most of us ordinary folk, for whom the helpful Google Maps voice assistant is our closest encounter with artificial intelligence. But then there are the real, everyday concerns like privacy and data security. Mostly, we have the sense to keep our pins and passwords to ourselves, and yet, as cybercrime becomes craftier and more persistent, there are massive organisations equally at risk to issues of data security. From common cybertheft to the extreme of cyberterrorism, our inextricable link with big data has the potential to turn on us all.

Data security vs data privacy

Confusingly, these terms are often used interchangeably, so let's clear up the difference. Data security refers to the processes an organisation puts in place to ensure that the data on their systems cannot be accessed and abused by unauthorised parties. Data privacy is what concerns us. It's the promise made by companies that any personal information entrusted to them will only be used as specified and agreed, and will not be shared without your permission.

Smartphones, for example, collect information about consumers' spending-related habits and are key contributors to the general data bank, tracking your media consumption, your geographical movements, social network and more. And, remember, in this integrated virtual world, all manner of computers, devices and machines are communicating and learning from each other too.

It's something of a love-hate relationship: some data-sharing we embrace with little thought to the consequences (think Instagram snaps), yet some invoke outrage at even an automated request for personal information. Big data is the fuel that powers this new revolution, so its collection is essential to healthy progress, and the World Economic Forum suggests that people may need to accept a trade-off, in which we agree to sacrifice a certain amount of personal privacy in exchange for the benefits of collectively gathered, analysed and responsibly utilised data.

Leading the way

In so many ways – unnoticed or obvious - this intricate web of artificial intelligence is making life better, saving us time and money, creating new opportunities and opening new doors. As drivers of economic growth and social progress, the best cities are nourished through innovative and technologically advanced infrastructure that enables them to flourish. Dubai's leadership, for example, has long embraced digitisation and the opportunities it presents to cement the city as a business and tourism hub. Its first Information and Communications Technology (ICT) strategy was announced as far back as 1999. Over the past two decades, Dubai has become one of the world's 'smartest' and most sustainable places, offering not only a super-efficient business environment but comfort and ease of daily living for its three million residents and many more visitors.

By harnessing the benefits of big data, Dubai is also ensuring a lighter load on the environment through enhanced infrastructure and sustainable use of resources. The Smart Dubai initiative, launched in 2014 and more recently updated to incorporate Smart Dubai 2021, develops and promotes technologies that support the vision of His Highness Sheikh Mohammad bin Rashid al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai, to make the dazzling city "the happiest city on Earth".

The success of Dubai 2021 is based on a holistic and studied approach, which used data to benchmark and inform its future.

Fast internet connectivity, and stress-free online access to and between all services, connected to the internet and monitored in real time, ensure an enriched city experience on all levels – from air quality and water supply, to smart government transactions and smoothly synchronised traffic flows, which in time, will include autonomous driving technologies.

Smart Dubai has also recently finalised a world-leading blue print of how the city's features can be made more efficient through blockchain technology. So much more than just the cryptocurrencies that rocketed it to fame, blockchain can be described as an independent, universally accessible ledger of every transaction, from hospital records to government data.

Peace of mind

Certainly, it is reassuring to know that Dubai's cyberspace is relatively well guarded. You can also gain control by empowering with knowledge about technological advances and by keeping attuned to news of the latest scams and organisational data breaches.

If you are concerned that your personal information may have been compromised by a company hack attack (as happened with Yahoo!), take these important steps to protect yourself:

- Assess the damage – Is it just a matter of a little-used email address, or might your vital information be at risk?
- Change your passwords on all affected accounts.
- Contact your bank – If necessary, block your credit card to prevent fraudulent spending.

Making Dubai the safest city in cyberspace

Supporting these technological strides is the Dubai Electronic Security Center (DESC), whose mission it is to ensure that strategic measures are implemented to safeguard sensitive and private information. This authority wants people to have the utmost confidence in accessing city services and conducting transactions online.

DESC's aim is to make Dubai the safest city in cyberspace. It is responsible for setting the benchmarks for best-practice security, with strategic plans that include initiatives to ensure cyber-resilience, and to combat threats, cyber-attacks and cybercrime.