REGIONAL BRIEFING: CYBERCRIME IN THE MIDDLE EAST AND NORTH AFRICA

This briefing is part of a set giving a snapshot of Middle East and North Africa consumer experiences across three key digital areas: privacy and data protection, cybercrime, and e-commerce.

The Middle East and North African (MENA) region is home to one of the most youthful populations in the world, with 60% of people aged under 30. It is undergoing a digital boom – internet access has almost doubled in the last seven years and now 71% of people are online compared to just 39% in 2012. Ambitious national strategies are supporting the roll out of 5G networks and the region has the fastest mobile phone growth rate outside Sub-Saharan Africa. There has also been an explosion in e-commerce.

We surveyed online consumers in the region[1], and found they are embracing this new digital world, with 75% of participants optimistic about the role of technology in helping them live a better life in the future.

However, we uncovered concerns about cybercrime that could hold back this potential. Cybercrime includes hacking, malware, online fraud, harassment and hate speech that spreads across computers and digital networks. Data breaches can expose consumers' names, phone numbers and emails putting them at risk of identity theft, financial fraud and harassment.

Consumer organisations can play a vital role in drawing attention to and reducing the risks of cybercrime for consumers, helping to create a safer and more trusted digital environment in the region that can bring empowerment, economic benefits and convenience.

How big a worry is cybercrime for online consumers in the MENA region?

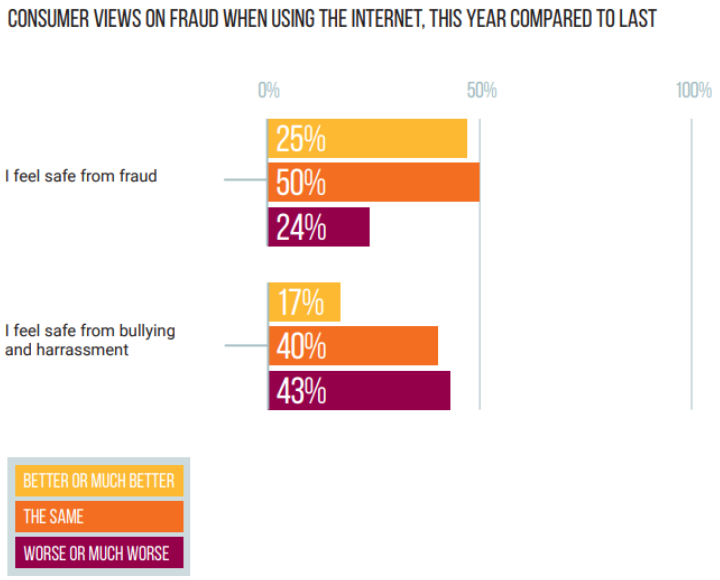
Cybercrime is the biggest source of concern for 81% of internet users around the world, including 76% of Middle Eastern and North African (MENA) consumers. The impact of cybercrime is felt across the region: 40% of online shoppers report that they have been victims of a cybercrime and 71% have witnessed or have been aware of a cyber-attack.

Our survey showed these concerns have grown over the past year - almost a quarter of MENA consumers we surveyed (24%) said they feel less safe from online fraud than they did the previous year, and 43% feel less safe from online bullying and harassment than they did a year ago.

Some MENA consumers are particularly vulnerable to cybercrime as criminals are attracted to the high wealth in certain countries. The United Arab Emirates (UAE), for example, home to some of the highest earning households in the world, is the second most targeted country for cybercrime, costing an estimated $1.4bn per year. Saudi Arabia has the highest global email spam rate and is

[1] *Consumers International surveyed 3,000 online consumers in Oman, Tunisia, Saudi Arabia and Egypt to help us understand MENA consumers' experiences with e-commerce, privacy and security online in a diverse range of markets. Survey findings were accompanied by interviews with our regional members.*

the fifth highest ranked country for email malware.



What are the effects of cybercrime on consumers?

Loss of data and risk of fraud: Apps that deliver anything from shopping to transport are rapidly developing in the region, but some of these platforms are already victims of security breaches that have exposed vast swathes of people's data putting them at risk of financial fraud. Hackers were able to reveal the personal details of 14 million users of Careem, a ride-sharing service in UAE, while in Saudi Arabia, five million consumers were affected by a security breach suffered by the popular directory app Dalil.

It's not just apps that are vulnerable to cybercrime. The Omani Association for Consumer Protection notes similar risks from online banking or consumer Internet of Things (IoT) devices. Some of these connected products, ranging from home security systems to wearable fitness trackers lack basic encryption and security, leaving them vulnerable to being taken over by hackers or exposing users' location, health or behavioural data.

Social media platforms also provide new ways for cyber criminals to target consumers with online scams. Several Arabic media personalities' social media accounts have been hacked, which has led to scammers tricking victims into sending money or harassing their contacts.

Consumers International research on the growth of social media scams also found criminals posing as authentic brands and reviewers to con consumers out of money. This not only damages the reputation of the individual being impersonated but can also lower consumers' willingness to trust the advertisements and promotions they view online.

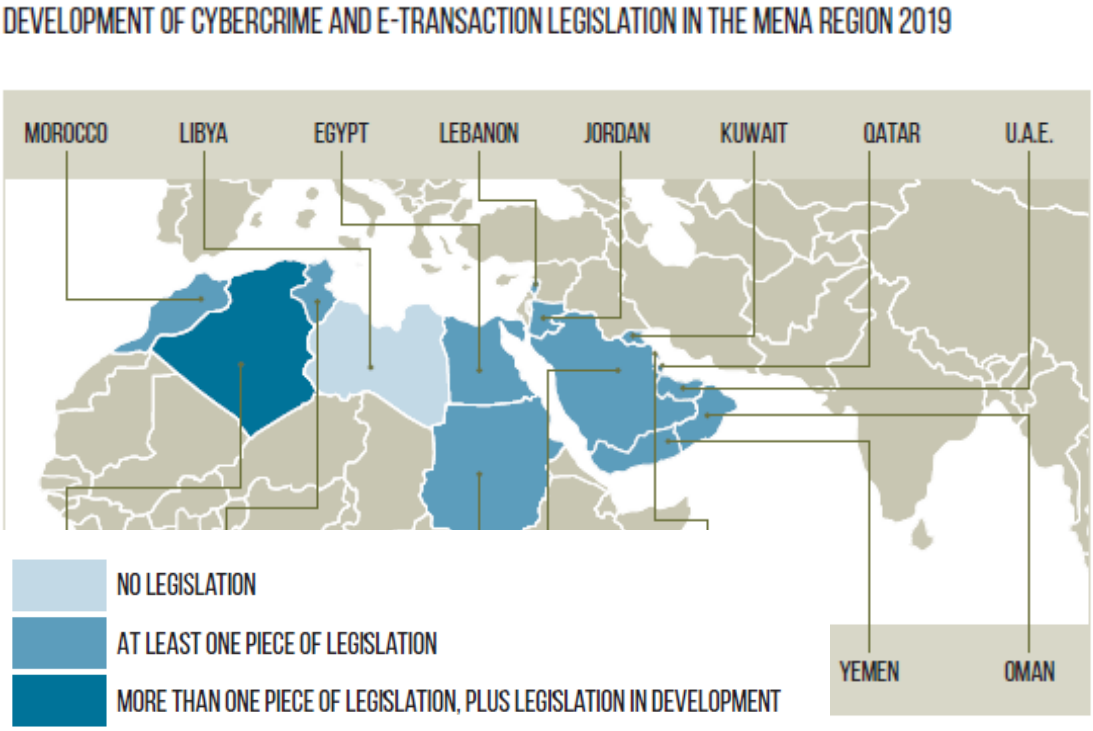
Economic costs: data breaches come at a considerable economic cost to consumers, governments and companies. Globally, the average cybercrime victim spends the equivalent of almost three full working days dealing with the aftermath of a cybercrime. Saudi Arabia and the UAE have experienced some of the costliest data breaches in the world – costing $5.97 million USD in lost business to organisations in 2017 alone.

"The information and advice consumers are getting is not enough to deal with the range of risks online."
Consumers Lebanon

Limiting online participation: Being a victim of cybercrime or hearing about it can make consumers feel less safe online, leading to consumers limiting the amount they participate with digital technologies. This has the potential to slow down adoption of helpful digital products and services that support financial inclusion, such as online banking or mobile payments.

What is the state of consumer protection for cybercrime?

Consumers need practical information from consumer authorities and online businesses, on how to engage safely with digital services. But improving consumer facing information may not go far enough – particularly as options for payments and interactions online grow as more and more consumer devices connect to the internet. Establishing system wide measures to prevent cybercrime is important and by building trust and participation, could deliver considerable benefits to consumers and the wider MENA economy.



According to the United Nations Conference on Trade and Development's (UNCTAD) Global Cyberlaw Tracker, most MENA countries (with the exception of Libya) have draft or existing laws in place to protect against cybercrime and facilitate safe e-transactions, such as the new Egyptian cybercrime prevention act. However, threats of data breaches, fraud and insecure online payments and websites suggest that legal protections not only have to evolve, but that enforcement should be prioritised. Initiatives led by our members on cybersecurity risks are also increasing consumer awareness of risks including:

- The Egyptian Consumer Protection Agency is warning consumers of how to protect themselves from potential security risks when shopping online, connecting to broadband and clicking through websites.
- In Saudi Arabia, the Consumer Protection Association launched a website in collaboration with the Ministry of Commerce and Investment to help consumers spot signs of online

fraud and learn more about how to protect themselves, with tools to report fraud via text message.
- The Omani Association for Consumer Protection is raising consumer awareness of fraud protection and personal safety online through seminars, courses and workshops.

Looking ahead, measures to create secure e-transactions and prevent cybercrime need to evolve to ensure consumers remain protected. For example, as consumer IoT grows in the region and the need for security increases, companies and governments can look to internationally agreed security standards that are already in development to guide best practice and future legislation.

What can consumer rights organisations do?

Failing to build and enforce strong security and anti-fraud measures in digital services (such as systems to monitor evolving threats, encryption and account authentication) can result in costly outcomes for consumers and the broader economy – and undermine consumer trust online. Consumer organisations in the region are well placed to make calls on governments and companies to improve the current situation.

Consumers International's recommendations to the G20 Consumer Digital Summit covered a range of actions governments and businesses could take to improve consumers' experiences online and help to build a trusted digital world. They included increasing access to the internet, security and transparency in terms and conditions, data protection by design, redress and education.

Below we have included the recommendations that are most relevant to cybercrime and security, alongside other actions that could improve security for consumers in the region drawn from our research into online scams:

Actions for governments and consumer protection authorities include:

- Prioritise and enforce measures to protect consumers' payment details, financial assets and personal identity against fraud or misuse.
- Engage with stakeholders to support the development of measures, including safe storage and transmission of financial data and any personally identifiable information.
- Establish and raise awareness amongst businesses of legislative requirements and how to facilitate consistent and effective fraud reporting to support decisive action against cybercrime.
- Require companies and governments to follow international best practice on storage and transmission of personal information.
- Establish breach notification rules for companies and clarify lines of responsibility.

Actions for online services and companies include:

- Adopt best practice standards for privacy and security by design, and use independent assessments of data security.
- Make it easy for consumers to adopt safe and secure practices.
- Manufacturers of consumer IoT products and services should follow guidelines to regularly assess cybercrime risks

"The more consumers feel secure in knowing their online transactions are protected, the more online participation will grow."
Egyptian Consumer Protection Agency

and review mitigation measures, as set out in the Consumers International Trust by Design guidelines and checklists.

- Companies should limit liability for consumers, developing compensation schemes in instances of security breaches or fraud and explore the potential of digital tools to detect fraud.

Actions for consumer organisations include:

- Explore the Consumers International Digital Index, a database of international examples of best practice in digital policies to protect consumers, to help inform approaches to working with regulators and policy makers and investigating consumer issues and complaints.
- Document consumer fraud to inform the design of targeted awareness-raising initiatives designed to reach vulnerable consumer groups, such as those with low digital literacy.
- Use our Trust by Design guidelines and checklists and explore how the security guidelines can be applied to different digital products and services.
- Develop digital awareness campaigns to build understanding of how consumers can take steps to keep themselves safe online and what to do if their data is lost or stolen.

This briefing gives a snapshot of the MENA consumer experience of cybercrime. See here for the accompanying briefings on privacy and data protection, and e-commerce.

Consumers International is currently building the Change Network, a powerful network of national consumer advocacy organisations and partners from business and civil society to explore how technology can provide solutions to some of the challenges faced by consumers around the world.

Together we will drive forward positive consumer outcomes on pressing issues such as artificial intelligence, the Internet of Things, e-commerce, data, sustainability, food and energy.

If you would like to be part of this growing network, please get in touch.

With thanks to:

Consumer Protection Association Saudi Arabia
Oman Association for Consumer Protection (OACP)
National Society for Consumer Protection of Jordan (NSCP)
Consumer Protection Directorate, Lebanon
Ministry of Economy & Trade
Consumers Lebanon
Yemen Association for Consumer Protection (YACP)
Consumer Protection Agency of Egypt, Ministry of Trade and Industry
National Federation of Consumer Associations of Morocco
Consumer Protection Association Libya
Sudanese Consumers Protection Society (SCPS)
National Union for Consumer Protection of Algeria

Methodology: Consumers International surveyed 3,000 online consumers in Oman, Tunisia, Saudi Arabia and Egypt to help us understand MENA consumers' experiences with e-commerce, privacy and security online in a diverse range of markets. Survey findings were accompanied by interviews with