اتحاد مصارف الإمارات
UAE BANKS FEDERATION

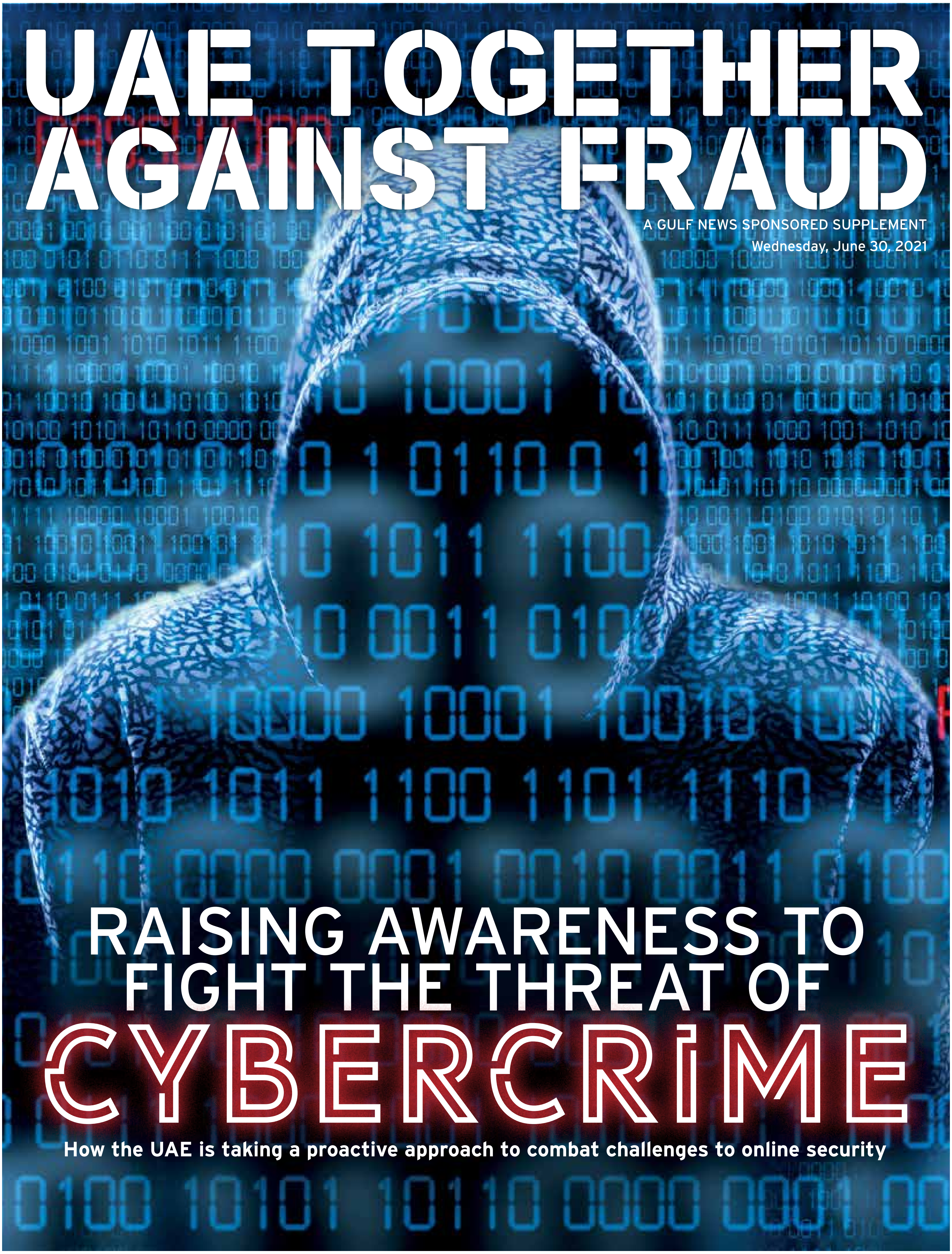
شرطة أبوظبي
ABU DHABI POLICE

TDRA هيئة تنظيم الاتصالات والحكومة الرقمية
TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

United Arab Emirates

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

FIGHT FRAUD



UAE TOGETHER AGAINST FRAUD

A GULF NEWS SPONSORED SUPPLEMENT
Wednesday, June 30, 2021

RAISING AWARENESS TO FIGHT THE THREAT OF CYBERCRIME

How the UAE is taking a proactive approach to combat challenges to online security

HOW TO PROTECT YOURSELF AGAINST THE THREAT OF CYBERCRIME

UBF's Fraud Awareness Campaign seeks to educate customers on cyber fraud risks and enlist them as allies in the fight against fraud

In April last year, UAE Banks Federation (UBF) launched the National Fraud Awareness Campaign, a wide-ranging initiative that aimed to educate customers to protect themselves from financial cybercrime and fraud, particularly in light of the increased use of digital banking services during COVID-19 pandemic. Being the UAE's first nationwide fraud awareness campaign, this joint initiative was organised by UBF in partnership with Central Bank of the UAE, Abu Dhabi Police, Dubai Police, and TDRA.

Through multimedia content – including articles, educational videos and social media posts – the campaign seeks to equip bank customers with the facts and tools they need to protect themselves against attacks. Encouraged by the overwhelming response that the campaign has received from citizens and residents across the country, UBF has recently decided to extend the campaign by one year, till the end of 2021, with a view to consolidate the successes of the campaign.

The threat of financial fraud has only increased in a world transformed by Covid-19

H.E. ABDULAZIZ AL-GHURAIR, Chairman of UAE Banks Federation

The nationwide campaign forms part of UBF's multi-faceted efforts to combat the growing threat of financial fraud, and was born out of the Federation's belief that customer awareness and education has a vital and indispensable role to play in keeping fraudsters at bay.

Commenting on the "#Fight Fraud" campaign, H.E. Abdulaziz Al-Ghurair, Chairman of UAE Banks Federation, said, "The threat of financial fraud has only increased in a world transformed by Covid-19, making it all the more essential for financial institutions to treat customers as allies in the fight against fraud. Raising customers' awareness about risky online behaviors and equipping them with the tools they need to protect themselves from attacks should be the first step in enlisting their support in the larger battle against fraud, and this remains the overarching objective behind our campaign."

JAMAL SALEH
Director General of UAE Banks Federation (UBF)

Jamal Saleh, Director General of UAE Banks Federation (UBF), said: "Customer vigilance remains one of the most potent forms of defense against financial fraud. Ensuring that customers have a good understanding of what constitutes fraud and how it can be tackled will empower them to take the right security measures against cyber intrusions and fraud and generally be more alert and aware when they are online."

#FIGHT FRAUD CAMPAIGN

Here we list some useful tips that together form the central pillar of our "#Fight Fraud" campaign, and which may help customers develop a clearer understanding of how to identify and avoid scams.

- **Phone Fraud:** Have you received a call from your bank asking for your personal information? This could be phone fraud. Always remember that your bank will never ask for your personal/financial information.
- **Email Fraud:** Do not respond to emails from unknown IDs & never click on any suspicious links or attachments. Ignore emails that create false urgency.
- **Social Engineering:** Stay a step ahead of social engineering scams. Never share your personal information with anyone over the phone, email, SMS, or social channels.
- **Advance Fee Scam:** Avoid communications that say you have won a lottery and ask you for an advance payment to claim the prize.
- **Business Email Compromise:** Watch out for emails that request fund transfer to a different account. This could be the work of a fraudster.
- **Bank Smart:** Don't give a chance to hackers or fraudsters to manipulate your mobile banking. Stay alert.
- **Shop Smart:** From choosing the right shopping website, to opting for the right payment mode, always choose secure ones.
- **Social Smart:** Keep your social accounts private as well as secure to protect your data from falling into the wrong hands.

GN FOCUS
A GULF NEWS SPONSORED SUPPLEMENT
SENIOR EDITOR PETER FEELY | HEAD OF CONTENT – SUPPLEMENTS AND CONTRACT PUBLISHING SANKAR SRI PILLAI
SENIOR ART EDITORS JOHN CATHERALL, NICHOLAS D'SOUZA | ASSISTANT ART EDITOR PRANITH RATHEESAN
BUSINESS SUPPORT EXECUTIVE FERMEL FUENTES | HEAD OF SALES – SUPPLEMENTS AND CONTRACT PUBLISHING SUNDAR GHOSH
SENIOR ACCOUNT GROUP MANAGER CHRISTINA REBELLO | PRE-PRESS SUPERINTENDENT SHAJI VARUGHESE
PRE-PRESS OPERATORS YOUSAF NAEEM, ATUL PARADKAR
CEO AND EDITOR-IN-CHIEF ABDUL HAMID AHMAD | DIRECTOR, SALES AND PUBLISHING ANSHUMAN JOSHI
PUBLISHER DAVID GEORGE | DESIGN DIRECTOR S.M. ARSHAD | PRODUCTION EDITOR FLOYD GONSALVES

DUBAI P. O. BOX 6519
EDITORIAL: 04 406 7688
ADVERTISING SALES: 04 406 7455
EMAIL: GNFOCUS@GULFNEWS.COM
ABU DHABI P. O. BOX 7441 TEL: 02 634 5144
PRINTED AND PUBLISHED BY AL NISR PUBLISHING LLC
DISTRIBUTED BY AL NISR DISTRIBUTION LLC

حماية
HIMAYA

كن يقظاً ..كن حريصاً
Be Security Smart, Stay Vigilant!

مصرف أبوظبي الإسلامي
ADIB

Share a smile, share kindness but not your password, no matter what!

Don't share your Password/OTP or PIN with anyone

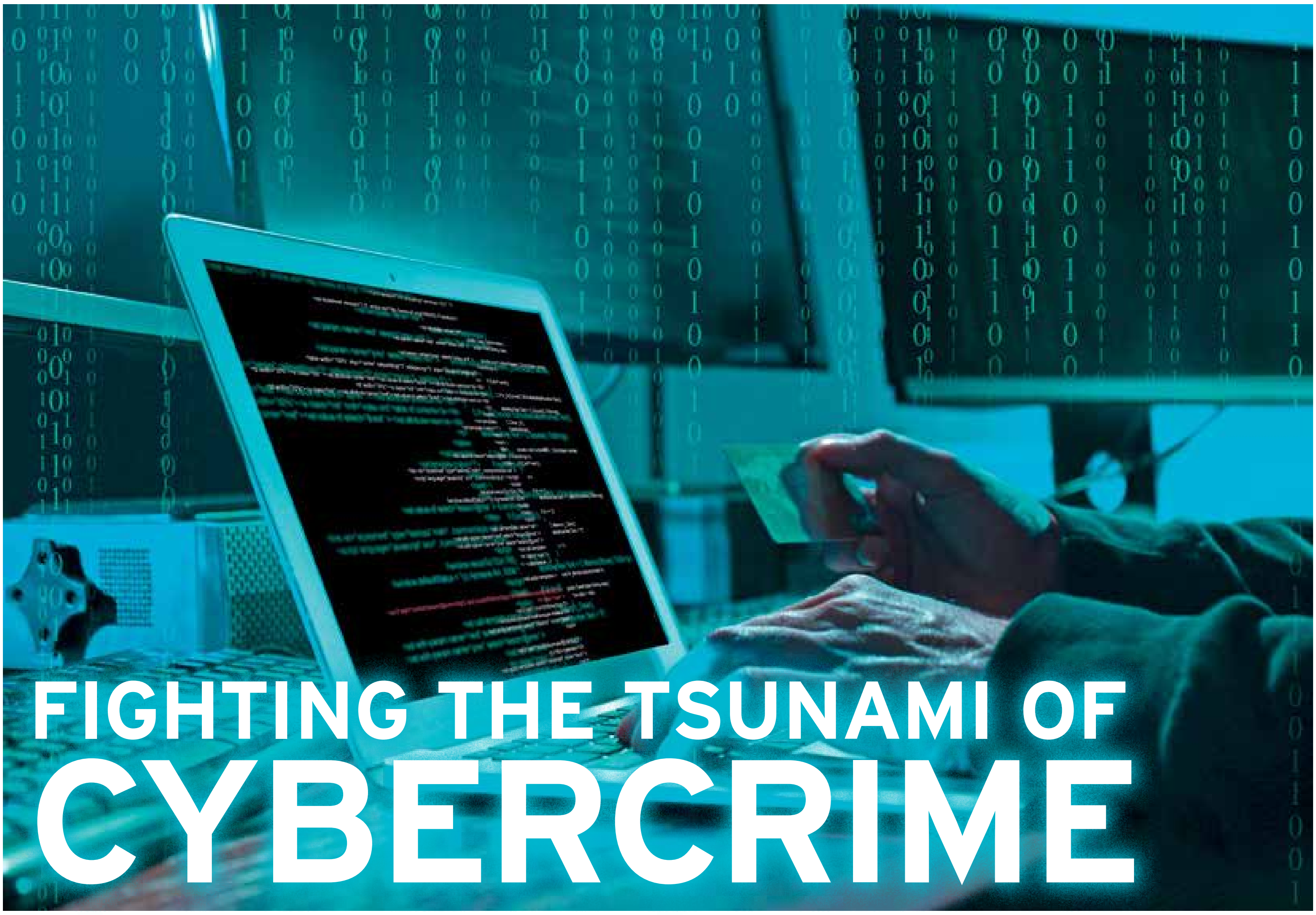
Change your Passwords and PINs regularly

Remember, ADIB will never ask for your Password/OTP or PIN

Stay one step ahead with your banking

DETECT. PREVENT. REPORT.

adib.ae | fb.com/ADIB | ADIB_bank | @ADIBTweets | ADIBStories | 600 543216



FIGHTING THE TSUNAMI OF CYBERCRIME

SHUTTERSTOCK

UAE banks take two-pronged strategy to battle against fraudsters

KEITH J FERNANDEZ
SPECIAL TO GN FOCUS

While the world was laid low by the coronavirus over the past year, a different kind of invisible plague has been spreading across the planet, with equally damaging after-effects. Dr Mohammad Hamad Al Kuwaiti, Head of Cyber Security for the UAE Government, likened the surge in online crime to a cyber pandemic.

"We saw a huge increase in [cyberattacks], at least a 250 per cent increase as we saw it here in the UAE," Dr Al Kuwaiti said during the Gulf Information Security Expo and Conference in Dubai in December, *Gulf News* reported at the time. "The financial sector was one of the most attacked, as well as even the health sector," he said.

The most common type of attack was phishing, where hackers pretend to be a trusted organisation such as a bank in order to extract sensitive information for financial gain. Such cons, which may take the form of genuine-looking emails or SMS messages and may feature banks' logos or link to official-looking websites, typically require bank log-in details, account numbers and access codes. Over the pandemic, such messages have been about fictional Covid-19 vaccines, the availability of oxygen units, pet adoptions, and even – cleverly – fabricated news of bank account hacks. Phishing emails surged by over 600 per cent in the first six months of the pandemic according to Dubai Future Foundation data.

Ransomware, where criminals block access to a victim's files in exchange for a financial payment by using malicious software programs that are downloaded via email or unsafe websites, was the other popular scam in the UAE last year.

Ironically, criminals were helped along by quarantines and lockdowns. As Dr Al Kuwaiti described it, individuals and organisations were unprepared for the abrupt shift to online schooling and work. Even as we spend more of our time online, often without adequate protection or over open public Wi-Fi, criminals have been able to exploit weaknesses in software and networks. The UAE is one of the world's most connected countries. Nearly all residents (99.15 per cent) have internet access, and the average time spent online is 40 hours per week, according to the *World Digital Report 2021*.

First line of defence

With criminals motivated by financial gain, banks have become the first line of defence in this digital war on crime. As UAE residents have adapted to social distancing measures and branch closures, fraudsters have likewise adjusted. "The UAE is a regional leader in digital adoption and e-commerce payments, and the Covid-19 pandemic accelerated that trend. Safety regulations and physical restrictions acted as a catalyst for transactions to move from malls to mobiles. However, the ensuing uncertainty has provided a fertile environment for cybercrime," AbdulAziz Al-Ghurair, Chairman of UAE Banks Federation, said in a recent statement. "While technology has helped our UBF member banks and their customers with tools for business continuity, it remains a double-edged sword with cybercriminals and attackers using ever more sophisticated tools. In such scenarios, customer awareness and education play a critical role."

ILLYAS KOOLIYANKAL
Chief Information Security Officer, Abu Dhabi Islamic Bank (ADIB)

Because of the nature of cyberattacks, where ordinary residents often unwittingly share confidential information with fraudsters, UAE banks take the view that prevention is better than cure in protecting against this tsunami of cybercrime. Nearly every bank in the country now sends out regular fraud awareness alerts and publishes detailed guidance on how account holders can protect

CONTINUED ON PAGE 6

A public service campaign by

Emirates NBD

In partnership with

شرطة دبي
DUBAI POLICE

DON'T MAKE A FRAUDSTER'S JOB EASY.

DON'T SHARE YOUR PASSWORD OR CVV.

DON'T DONATE MONEY WITHOUT VERIFICATION.

DON'T SHARE YOUR BANK ACCOUNT DETAILS.

Media partners

البيان B4U B4U أفلام CHANNEL 4 Radio Network الإمارات اليوم إمارات FM الاتحاد Khaleej Times

GULF NEWS الخليج ENG HILLS ADVERTISING L.L.C Radio 1 Radio 2 Star FM facebook

SHUTTERSTOCK

CONTINUED FROM PAGE 4

Fighting the tsunami of cybercrime

themselves while browsing or shopping online.

Now banks are teaming together with the police to raise awareness of online cyber traps and how residents can easily be conned. The UBF joined with the Central Bank of the UAE (CBUAE), police in Abu Dhabi and Dubai and the telecommunications regulatory authority to run a series of national campaigns, reminding the public to stay vigilant against phone calls and messages, while emphasising the importance of not disclosing personal and banking information to any person or entity.

In February, Emirates NBD launched an online education campaign centred around a shareable film and social media posts where a fictional fraudster – complete with fake Instagram account – masqueraded as a representative of legitimate organisations to steal sensitive information.

Technology as a weapon

In parallel, the bank has strengthened its security technologies through the use of biometrics, contactless identity verification and secure encryption. Last July, it migrated its customer base to a new Smart Pass service, where customers can authorise digital transactions by keying in an instant token or personal identification number (PIN) that is generated within their banking app. The service protects against mobile SIM card swap fraud by doing away with the need for SMS-based one-time password (OTP) authorisation. Similarly, its TruID solution enables new customers to have their identity documents verified using contactless near-field communication (NFC) technology when opening an account through the bank's mobile app.

"Customer safety is our top priority, and we are constantly developing new ways to make banking more secure, convenient and hassle-free," said Suvo Sarkar, Senior EVP & Group Head, Retail Banking and Wealth Management, Emirates NBD. "As fraudsters develop increasingly sophisticated means of accessing personal information, our technology-driven security solutions help safeguard consumers in today's digital age so that they can conduct banking securely and easily, from anywhere in the world."

Other banks have also stepped up their embrace of technological weapons to deal with these increasingly complex cyberattacks.

The Abu Dhabi Islamic Bank (ADIB), which has also rolled out a joint campaign with security authorities, is now focused on increasing its monitoring capabilities, as well as implementing additional layers and types of controls to support a new set up that aggressively adopts cloud and remote access services.

> “
> We have elevated 24X7 monitoring to timely detect and respond to potential malicious activities.
>
> **ILLYAS KOOLIYANKAL,**
> CHIEF INFORMATION SECURITY OFFICER, ADIB

The bank has strengthened its technical, procedural and security awareness controls while enhancing its secure remote connectivity services to cater to different kinds of users, and is leveraging various technologies by moving from on-premises tools to cloud based technologies.

"ADIB has introduced a new secure set of collaboration tools and digital channels to enhance business productivity and customer experience without compromising information security," Illyas Kooliyankal, Chief Information Security Officer at Abu Dhabi Islamic Bank (ADIB), told GN Focus.

"We have elevated 24X7 monitoring to timely detect and respond to potential malicious activities."

"Through a progressive strategy, ADIB will continue to ensure tighter security measures and controls are in place, ensuring staff are fully aware of its work-from-home policies and practice secure working, while updating the bank's readiness plan to meet all potential scenarios," Kooliyankal said.

Whether these steps are enough to stem the tide of crime remains to be seen, but as in most other situations, staying alert is the first step to staying safe.

PARTNER CONTENT

STAYING ONE STEP AHEAD OF CYBERCRIMINALS

How Mashreq works diligently to protect its customers

KARTIK TANEJA, HEAD OF PAYMENTS AT MASHREQ

How does Mashreq work to ensure it's always one step ahead of cybercriminals?

I think "one step" is a very good choice of words. Cybercriminals keep coming up with creative new ways of doing fraud, and the banks have to keep employing even more creative ways to overcome them. At Mashreq, we use a combination of global best practices, expert advice from Mastercard/Visa, our in-house learning from the cases we've seen, as well as learnings shared by law enforcement or other authorities.

We are also working on new-age solutions like biometrics, risk-based and step up authentication, which ensures customers enjoy frictionless payments, while being protected from fraud.

I would like to share the latest innovation we have done to protect our customers. It's simple, but we are confident it will be very effective:

Over the past few months, we noticed a new trend of fraud where a customer intends to make a small payment at what seems like a genuine, functional website. It could be Dh10 for an international courier delivery, or Dh20 for a great deal at a well-known pizza brand. But what's happening at the back end is that the websites are run by fraudsters and they use the website to steal one-time passwords and conduct unauthorised transactions.

What did we do? We revised our OTP SMS format so that it also includes the transaction amount, the merchant name, and OTP in that order. The layout (intentionally) is such that customers will be forced to read the amount and the merchant name before they see the password. We are confident that this will reduce frauds as customers notice that the amount and merchant is not what they intended it to be. This new format should become industry standard soon, until the region moves on to soft tokens or other risk-based solutions

What does Mashreq do to promote security awareness for its customers?

We keep our customers aware by a) being transparent and b) keeping them aware. We constantly educate our customers on the importance of keeping their financial details safe, educate them on how to protect themselves from various evolving fraud trends, and what to do when they suspect fraud:

1 Mashreq is a key participant and contributor in the UAE National Fraud awareness campaign run under the leadership of UAE Central Bank, UAE Banking Federation, Abu Dhabi police and Dubai police.

2 We are not afraid of transparently telling our customers exactly how a transaction dispute works. "Was it an ecommerce transaction without 3D secure password? No problem you will get all your money back". "Was it a 3D Secure transaction with a password? Well, unfortunately it seems like you have been tricked into sharing the password, the liability will be with you". We believe in transparency of information with our customers when it comes to their rights and liabilities in a disputed transaction. We are the only bank in the region and one of the very few banks globally which clearly informs customers of the liability in various types of transactions. Customers can visit Mashreq.com/ccdisputeform for a detailed snapshot of the same.

We are working on new-age solutions like biometrics, risk-based and step up authentication, which ensures customers enjoy frictionless payments, while being protected from fraud.

3 A monthly "anti-fraud tips" email and SMS is sent to the customers to assist them in their role in not becoming a victim of fraud.

4 We have a dedicated page on our website which is a collection of best practices of online security and card safety tips, which can be accessed at Mashreq.com/onlinesecurity and mashreq.com/cardsafety.

5 The last thing anyone wants when disputing a transaction is to have to go through difficult paperwork. We now offer paperless transaction dispute (no print, no signature). Customers can download a PDF form and email it to us.

6 We understand our customers' need to travel with peace of mind. Our Mashreq Mobile App offers a range of controls that customers can access instantly:

- Temporary card block
- Set and Reset of PIN
- Block and replacement of the card
- Set-up transaction limits
- Set -up daily limits
- Set no. of transactions per day
- Block countries
- Block merchant categories

"Mashreq ensures that our customers enjoy the most convenient financial services. Our values include being passionate about clients while being socially responsible and transparent. We are committed to protecting our client's financial security," said Taneja.

COMMON INCIDENTS OF FRAUD IN THE UAE

Insights into how to avoid falling victim to fraudulent activity

GURCHARAN CHHABRA
HEAD OF FRAUD PREVENTION & INTELLIGENCE, MASHREQ

Gurcharan Chhabra, Head of Fraud Prevention & Intelligence and a veteran at Mashreq, has been at the forefront of Mashreq's war against fraud. As per his experience, these are the types of fraud to that customers are subjected to nowadays:

- Fraudsters who pretend to be Bank staff call customers under a (fake) high pressure scenario (e.g., "Your card is being used abroad right now for USD3,000. I urgently need some information to block it"). These are fraudsters trying to obtain sensitive financial information or 3D Secure passwords.
- Fraudsters ask for sensitive information while pretending to be from your financial institution, law enforcement, police, Central Bank or immigration.
- Fraudsters send emails/SMS to customers while disguised as courier companies, asking them to share card details online
- Fraudsters advertising "50 per cent off on Pizza" or any other such promos, again with fake websites attempting to steal customer information

Customers can protect themselves from fraud by following these best practices:

1. Do not respond to unknown or unsolicited calls.
2. If you are told of a critical action on your Bank account or card, do not panic and share information. Call your Bank on their registered phone number and ask about your account/card.
3. Do not share any confidential information, Password, PIN or OTP with anyone over the phone or otherwise.
4. Double check the "amount value" of your transaction given in the OTP, before inputting it for a card transaction
5. Avoid clicking on links. Whenever possible, type in the URL yourself. If clicking a link is unavoidable, watch the top row of the browser carefully to make sure the URL is of the right website
6. Carefully monitor transaction SMSs and emails sent by the Bank and, in case of any issues, reach out to the Bank immediately to ask for card blocking (Mashreq customers can also instantly place a temporary block on the card through the Mashreq-Mobile application).
7. If you suspect a fraud, file a dispute with the Bank as soon as possible. Mashreq customers can access our digital dispute form at mashreq.com/ccdisputeform. Mashreq works diligently with stakeholders, including payments schemes, to maximise the chances of successful dispute refunds.

TAKING A SATIRICAL APPROACH TO CONSUMER AWARENESS

How Emirates NBD has launched engaging and amusing campaigns to fight fraud

As a leading bank in the UAE, Emirates NBD has taken an active role in raising consumer awareness on safe, secure banking.

The bank has conducted widely acclaimed security-related significant campaigns, in cooperation with the country's law enforcement agencies, designed to engage customers in a fun, memorable manner.

The centre piece of Emirates NBD's #SecureYourAccount campaign was the *It Wasn't Me* video reminding customers that the bank would never ask for personal details such as online or mobile banking credentials and password, card PIN or the three-digit CVV number on the back of the card and to remain vigilant about fraudulent emails, links, websites or calls to protect themselves against potential fraud.

The follow-up campaign addressed fraud and online security to educate the public on how to identify and protect themselves against highly deceptive tactics fraudsters employ. At the heart of the campaign was a shareable, social satire comedy film, *How To Grow Rich During The Pandemic*, showcasing the lavish lifestyle of a fictional fraudster named James Jefferson playing different roles as he impersonates legitimate organisations via various means in order to steal sensitive information, with the serious message "Don't Make the Fraudster's Job Easy." The film was accompanied by a stealth social media campaign following the outrageous life of James Jefferson via his Instagram handle @ jjj_jefferson who was finally revealed as a fraudster. Emirates NBD also conducts regular SMS and email campaigns as well as posts messages across its social media platforms to sensitise customers to potential phishing and vishing attempts by fraudsters and remind them to never share their personal details with anyone.

The bank is currently running a live Spot the Fraudster, moderated by popular radio host, Kris Fade, every Tuesday at 8pm across its social media channels, designed to engage and educate on the different persona adopted by fraudsters.

The UAE authorities and Emirates NBD urge members of the public to report suspicious links or emails related to their bank accounts to their respective bank's call centre and Dubai Police. Emirates NBD customers can contact the bank's call centre on 600 540 000 and Dubai Police through their website: *www.ecrime.ae*

THE SAFEST PLACE TO BANK. YOUR HOME.

Use the RAKBANK Digital Banking App or Online Banking - it's easy, secure and available 24x7.

To stay safe, always remember as a bank, we will never ask for sensitive information like your Digital Banking User ID or Password, Credit/Debit Card Number, CVV, PIN or OTP.

Kindly report any suspicious activity
immediately to contactus@rakbank.ae
or to our Phone Banking unit on 04 213 0000

RAKBANK
Simply Better

5 COMMON TYPES OF BANK FRAUD IN THE UAE

What to look out for if you want to avoid compromising your personal details

BY KEITH J FERNANDEZ
SPECIAL TO GN FOCUS

Even as the novel coronavirus continues to mutate into ever more dangerous forms, hackers and fraudsters have similarly stepped up their efforts to parting unsuspecting UAE residents from their money with financial scams. Several new variations on established dodges have made their way to the UAE this year, from cryptocurrency counterfeiters to Expo 2020 Dubai imitation rackets. As cybercriminals take advantage of the pandemic, global digital fraud attempts rose 149 per cent from January to April this year as compared to the previous four months, consumer credit reporting agency TransUnion reported recently.

Here's how some of the latest scams have played out in the UAE over recent months and how to handle them. In all cases, if you've shared any confidential financial information, immediately report your actions to your bank and to the police.

THE EMIRATES POST EMAIL TRAP

In March, Emirates Post posted on social media that fraudsters were sending fake emails in its name, asking recipients to reveal personal information such as passwords or bank details. It advised UAE residents not to respond to these emails.

This type of social engineering attack, called phishing, dupes victims into opening emails or SMS and text messages where they are asked to share confidential information. Such bogus emails may appear to come from banks, big-name brands or other organisations.

How to avoid it: Don't open unfamiliar emails or text messages – the subject line is usually a giveaway, and email providers often mark emails as spam. If you do, flag the message as spam. Then disconnect your device from the internet and any networks it may be linked to and run an antivirus program. Then log on again and change all your password details.

THE FAKE UAE CENTRAL BANK CALL

This month, authorities in Abu Dhabi warned of deceptive phone calls from hucksters pretending to represent the UAE Central Bank. The callers asked victims for their bank account details or having already obtained these through other methods, for One-Time Passwords. This is typical of vishing, a type of voice phishing call where victims are targeted with personalised communication messages. Other examples include calls from people pretending to be bank officers, lottery officials, Expo 2020 Dubai organisers or representatives of well-known brands.

How to avoid it: Don't take calls from unfamiliar numbers. If you do, hang up immediately. Conduct an independent web search to verify the offer or issue and visit the organisation's website.

THE DUBAI COIN DODGE

In May, Dubai's government flagged up that the relaunch of Dubai Coin, a counterfeit cryptocurrency that was being peddled as a digital payment option online and in stores, which had no official backing. The cryptocurrency had been used for a trial in 2017 and later shelved, but in its new avatar it was an example of domain spoofing, a type of phishing attack where you click on what appears to be a legitimate webpage but is actually a malicious site. In this case, the scam drove the coin's value from below $0.09 to $1.13 within two days. Similar fake domains purportedly represent Amazon, Google and even the UAE government.

How to avoid it: Watch for misspellings, look for the lock icon next to the website URL and only share the bare minimum. Triple check any emails that look like they're from retailers, including courier and delivery notifications.

THE SIMPLE SIM SWAP

Has your phone suddenly gone dead? Or perhaps you've lost your network? Your account could have been compromised by SIM card fraud, where a fraudster obtains a replacement SIM card of a registered mobile number and fake identity documents or information from social media. They then transfer money via online banking services or takeover your social media accounts. This sort of account takeover fraud has declined to almost zero since mobile providers now require customers to request a replacement SIM card in person with their original Emirates ID and fingerprint verification.

How to handle it: Contact your mobile provider, your bank and the police. From another device, log on to social media and any applications you may use and change your password.

THE COVID-19 CURE INVESTMENT CON

Last year, the Central Bank of the UAE spoke of how coronavirus scammers were contacting residents via email, text messages, phone calls and home visits to discuss investing in a cure for the novel coronavirus, in a medical equipment production centre, in insurance protection or towards investments or charity. Such fraudsters asked for credit cards details, cheques or funds in a form of outright theft.

How to handle it: Never provide cash, credit cards or personal information without verifying the details of the vendor. Check their trade licence and registration papers. If something sounds too good to be true, it probably is.

COULD BIOMETRICS BE THE FUTURE OF SECURITY?

SHUTTERSTOCK

Earlier this month, the country's first authentication solution for e-commerce transactions was introduced in the UAE

GN FOCUS REPORT

This month, Abu Dhabi Islamic Bank (ADIB) has announced it partnered with Visa to introduce the UAE's first biometric authentication solution for e-commerce transactions. The solution leverages Visa Consumer Authentication Service to deliver a significant improvement in customer experience and reinforced data security.

Visa Consumer Authentication Service aims to enhance user experience, as well as mitigate security and fraud risks by replacing traditional verification methods, such as OTP requirements, with biometric authentication using fingerprint and facial biometrics.

Once the solution is implemented, ADIB customers can authenticate their e-commerce transaction by using their ADIB Mobile application biometric authentication instead of the conventional OTP that is sent by SMS or email. Unlike conventional procedures for user authentication, biometrics makes it difficult for intruders to use illegally obtained consumer credentials, allowing for stronger security and a time-efficient experience, even when the customer is travelling.

Philip King, Group Head of Retail Banking at ADIB, said, "Due to the pandemic, online security and fraud protection has become more essential than ever. e-commerce websites have to confront various security issues from online fraud to theft of confidential data. Unlike conventional authentication processes, a biometric identification system uses the physical characteristics of an individual to grant account access, ensuring the security of consumers. Through our partnership with Visa, we aim to continue evolving our approach to using digital solutions to improve our customers' experience."

Shahebaz Khan, Visa's General Manager for UAE, stated, "Our Consumer Authentication Service is an example of how Visa's network intelligence can create tangible value for our bank clients and merchants. Because the solution only prompts consumers for verification of the riskiest e-commerce transactions, most consumers will have a streamlined authentication process. Consumers in the UAE are savvy and with more transacting online, Visa's biometric solution for ADIB offers them the safe and optimal online payment experience they increasingly expect. We are delighted to see ADIB become the first bank in the UAE to launch biometric authentication for e-commerce transactions."

—WAM

What are biometrics?

Understanding the technology, its advantages and disadvantages

PETER FEELY
SENIOR EDITOR

If you're the owner of an iPhone, there is a strong chance you may be immersed in the world of biometrics. The 30,000 infrared dots, which are projected on to the user's face as part of process to unlock their phone with Face ID is one of the most widely known examples of biometric security. Apple claims it is so accurate and secure, the risk of mistaking the owner's identity is one in a million. Other types of biometric security, aside from facial recognition, include voice recognition, fingerprint scanning, iris recognition and heart rate sensors.

According to internet security giant Kaspersky, "Physical characteristics are relatively fixed and individualised — even in the case of twins. Each person's unique biometric identity can be used to replace or at least augment password systems for computers, phones, and restricted access rooms and buildings."

The company says that biometrics are commonly categorised in three groups: biological biometrics, morphological biometrics and behavioural biometrics.

The biological group use genetic and molecular information such as a person's DNA and can often be assessed through an individual providing a fluid sample. The morphological group is associated with structures within someone's body, such as their iris, fingerprint or the shape of their face, as is used in Apple's Face ID system.

The third, behavioural group, maps people's unique patterns and characteristics such as how they walk or speak. It can even be used to identify people based on the way they type on a keyboard.

The advantages of using biometrics is that they are more difficult to steal or impersonate in comparison to traditional passwords.

One concern surrounding biometrics is privacy, with people worried that their private data can be collected and used without their consent. Facial recognition is already being used throughout the world in cities such as New York, Moscow and Shanghai, where police are using the technology to help solve crimes.

Another concern is the potential for cybercriminals to steal people's biometric data. One such example happened in 2015, when data on the fingerprints of 5.6 million government employees was compromised following a breach at the US Office of Personal Management.

"The Free for Life"
Card that frees up your life.

Limited Offer | T&Cs Apply

البنك العربي المتحد
UNITED ARAB BANK

@uabuae | uab.ae | 800 474

SHUTTERSTOCK

Addressing the threat of ransomware

Why you should vaccinate your devices as well as yourself

GN FOCUS REPORT

BARRY COOK
Privacy & Group Data Protection Officer, VFS Global

The coronavirus pandemic triggered a wave of digital transformation with companies across the globe bring their businesses online. While this has opened new opportunities for businesses, the pace or transformation has resulted in an increase in cybercrimes as attackers continue to take advantage of our greater reliance on the virtual world. Now that organisations are planning and implementing their recovery strategies, there is one form of business that has exploded - the creation and use of malicious software. Users across the world have fallen victim to cybercriminals. The most common attack being that of Ransomware. While Ransomware is nothing new, the ways in which it is being used and spread is.

The change from in-person meetings to online video-conferencing calls was exploited by cybercriminals to launch ransomware attacks by crashing video calls and baiting users with malicious domains proponing to be the video conference company. Of course, the links on the fake domains download malware. A significant new cyber-tactic that has emerged is 'double extortion'.

Ransomware occurs when a hacker blocks access to a victim's files, then demands payment to restore access. New research by TrendMicro, says critical public infrastructure and government IT systems were becoming a primary focus for hackers globally, with ransomware being their preferred weapon of choice.

The pandemic itself created new challenges to digital privacy. Governments and organisations employed digital contact tracing in an attempt to contain outbreaks. This presented a new challenge for privacy professionals. Can we have effective contact tracing while maintaining personal privacy? With the number of contract training schemes that were scrapped or extensively redesigned then it would be safe to assume the answer to that question is "probably no."

Your Device Needs Vaccination Too

The vaccine that can help protect your devices is patch updates. These patch updates contain fixes for known exploits and vulnerabilities on the device they are updating.

It is recommended by manufacturers that patch updates should be set to automatic in order to automatically update and protect your devices. Similar to how the Covid-19 vaccination does not guarantee a 100 per cent protection, device vaccination also goes only so far, but it does not mean you should not attempt to protect your devices.

Additionally, the most effective step is to be prudent while using your devices and not blindly clicking on the "OK" button or link when random pop-ups appear on the screen. Being attentive and mindful has been proven to avert most attacks and prevent you from becoming part of the chain of compromise. This is the digital equivalent to washing your hands and wearing a mask!

For organisations, cybersecurity is even more important as most employees today are connected from homes using their home Wi-Fi networks that may have weaker protocols. This not only makes devices directly vulnerable, but also exposes them to hacks on other personal devices connected on the same network, such as mobile phones, digital assistants, smart appliances, gaming machines etc. pre-empting, preparing, and spreading awareness will go a long way in reducing risk.

While staying home and being virtually connected does help keep one in staying physically safe from Covid-19, it can increases the chances of becoming a cybercrime victim. So, break the chain and protect your personal devices to avoid getting hit by a virus of a different kind.

VIGILANCE IS ALL YOU NEED TO DEFEAT CYBER THREAT

Stay Alert!

As we witness a massive shift from the physical world to the virtual one, our dependencies on digital platforms have increased drastically. Be it online purchases, virtual meetings, banking transactions or business webinars, we must be alert now more than ever.

As banking connects you across devices, platforms, and channels, National Bank of Fujairah empowers you with various digital security features to mitigate fraud, including the most advanced multi-factor authentication systems, such as biometrics and facial recognition. We remain vigilant and will continue to maximise security to safeguard the ever-evolving technological advancement, addressing your growing banking needs.

8008**NBF**(623)

nbf.ae

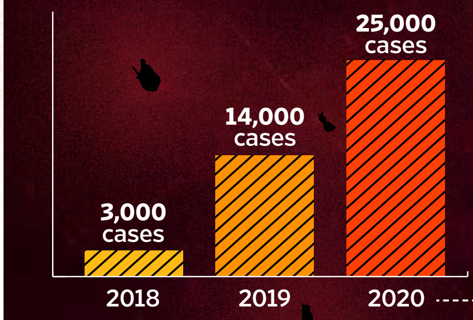
nbf

In good hands

CYBERCRIME In the UAE

Facts and figures about the digital landscape in the country

E-CRIMES REGISTERED WITH DUBAI POLICE



300% increase in cyberattacks

MOST COMMON FORMS OF CYBERCRIME

Phishing

Ransomware

AVERAGE UAE RESIDENT SPENDS

7.24 hours online each day

97.6% residents own a smart phone

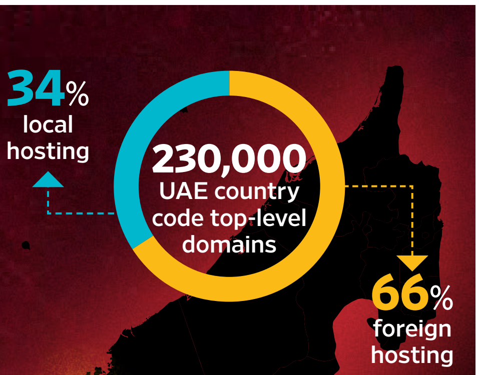
99% are active on social media

BIGGEST GLOBAL DATA BREACHES IN HISTORY

- **2013** Yahoo lost data from 3 billion accounts
- **2017** Equifax compromised the information of 143 million consumers, costing the business more than US$4 bn
- **2018** Under Armor's MyFitnessPal app was breached, affecting 150 million users
- **2018** Marriott-Starwood compromised data from 500 million customers

MAJORITY OF UAE

COMMERCIAL, GOVERNMENTAL, EDUCATION ORGANISATIONS HOST WEBSITES OUTSIDE THE UAE



34% local hosting

230,000 UAE country code top-level domains

66% foreign hosting

UAE is the 3rd most attractive target for cybercriminals after Sweden and Iceland

2020

49% of UAE companies have experienced a ransomware attack

1.1 million+ phishing attacks

Cost US $1.4 bn

249,955 vulnerabilities found

3.7 average vulnerabilities found per website

AFFECTED COMPONENTS

5%	16%	66%	12%
application server	network server	web application	web server

15% of affected components are unpatched IoT devices

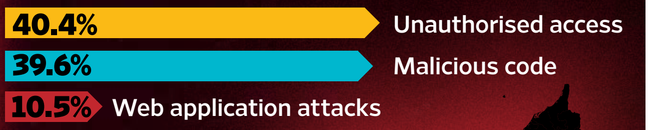
1 business is hacked every 3 seconds

FREQUENTLY FOUND WEAKNESSES

Missing Microsoft Windows Operating System patches

47% reuse the same password

COMMON INCIDENT TYPES



40.4%	Unauthorised access
39.6%	Malicious code
10.5%	Web application attacks

80% of data breaches are related to the use or loss of stolen credentials

4.27% of the world's ransomware attacks take place in the UAE

November 2020 UAE Cabinet established the UAE Cybersecurity Council

COST OF A DATA BREACH IN UAE AND SAUDI ARABIA

Rose by 9.4% in 2020 to **US$6.53 million** on average

Global average is **US$3.86m**

INFOGRAPHIC: PRANITH RATHEESAN; SOURCES: CYBER RESILIENCE REPORT - UAE THREAT LANDSCAPE 2021 - THE DIGITAL14; WORLD DIGITAL REPORT 2021

BANKING FRAUD AWARENESS AND PREVENTION

Why it is imperative to dedicate substantial resources to secure infrastructure

ILLYAS KOOLIYANKAL,
CHIEF INFORMATION SECURITY OFFICER, COO-GISD-GROUP INFORMATION SECURITY DEPARTMENT, ADIB

ADIB believes that it is imperative to dedicate substantial resources not only in building a secure and resilient infrastructure, but also improving capabilities amongst people and processes.

ADIB uses state-of-art technologies and multi-layered security solutions to protect customer information and constantly evaluates, develops, and implements advanced banking security measures.

The bank also introduced a secure set of collaboration tools to increase business productivity without compromising information security. In addition, the bank also enhanced its technical, procedural and security awareness controls, increased the portfolio of secure remote connectivity services to cater to different kinds of users, and leveraged various technologies by moving from on-premises tools to cloud based technologies.

ADIB is focused on increasing its monitoring capabilities, as well as implementing additional layers and types of controls to support a new setup that aggressively adopts cloud and remote access services. Through a progressive strategy, ADIB will continue to ensure tighter security measures and controls are in place, ensuring staff are fully aware of its work-from-home policies and practice secure working, while updating the bank's readiness plan to meet all potential scenarios.

The bank rolled out training sessions to ensure that employees are well-prepared for cybersecurity risks. In addition, ADIB also established reliable teams at call centres who can help customers with issues on unusual and suspicious transactions.

Meanwhile, in order to reach and educate customers on cybersecurity and fraud attacks, ADIB executed several educational and awareness campaigns in collaboration with Visa, Dubai Police, Abu Dhabi Police, and the UAE Bank Federation to reach and educate customers on cybersecurity and fraud attacks.

ADIB constantly develops its approach to ensure that it effectively monitors, predicts, and prevents risks, threats, and suspicious activities. This means a continuous review of the bank's risk strategy and making investments for cyber resilience.

THE IMPORTANCE OF INVESTING IN CYBERSECURITY

Why protecting customers' online information should be a priority

ALEXANDER THOMAS
CHIEF RISK OFFICER, UNITED ARAB BANK (UAB)

What steps does UAB take to protect its customers' details and information?

In consideration of the criticality of the customer data, the protection of the customer's data is of paramount importance for UAB and its management.

UAB has invested substantially on improving the cybersecurity posture of the bank and adapts to various emerging threats, while designing the controls. UAB's proactive (24x7) security monitoring reinforced with cutting-edge security technologies from End-point to Gateway level supports to protect customer's data from any intrusion.

The data sent across in various channels are encrypted and ensure only need-to-know access are provided. Moreover, UAB conducts periodic security tests to ensure any new vulnerabilities have been identified and fixed in a timely manner.

UAB is currently in the process of getting Payment Card Industry Data Security Standard (PCI-DSS) certification and are in compliance with other various local and international security standards.

How does UAB ensure it works to counteract evolving incidents of fraud and deception?

Fraud attempts continue to adapt with the evolution of technology. There has been an increasing trend from fraudsters who use social engineering techniques to attempt to defraud individuals via the scams for example; one time password scams, intrusion of business emails, breach of personal information and mule accounts.

Digitalisation represents great opportunities as well as responsibility for banks towards their customers and regulators. The bank is vigilant to respond to new threats and is continuously embracing the new approaches and technologies to prevent and detect fraud and has developed a robust mechanism to prevent, detect, monitor and respond to the emerging fraud risks. Moreover, the Bank has instilled the culture of continual fraud risk awareness internally and to customers by providing them perpetual cybercrime and fraud awareness messages (via SMS, social media, on our website and at ATMs) to protect themselves from financial cybercrime and fraud.

What comfort does UAB offer its new customers against fraud?

The bank is committed to protect our customers from fraud threats and trends by unremittingly embracing the new approaches and technologies to prevent and mitigate these fraud risks. The bank has the fraud risk prevention, detection and monitoring mechanism to cater to the evolving risks of fraud. The bank has also been actively participating in national fraud awareness campaigns by enlightening the customers with the new fraud threats and trends to safeguard themselves from being the victims. Moreover, UAB facilitates customers to report suspected or actual fraud incidents to the bank through its channels.

A VIGILANT APPROACH TO ONLINE BANKING

There are several steps that can be taken to reduce the risk of falling victim to online fraud

K.S. RAMAKRISHNAN
CHIEF RISK OFFICER,
RAKBANK

What are the main pieces of advice you give your customers to help protect them from fraud?

Cyberattacks, financial crime, and fraud are becoming increasingly more targeted, intricate, and persistent. While technologies have made advances in risk management, cybersecurity, and fraud prevention, we always advise our customers to take additional precautionary measures.

Firstly, always use your own computer or use a trusted computer for banking purposes. We advise that our customers avoid using a shared or public computer when it comes to banking. Ensure that your computer is equipped with antivirus and a firewall to prevent any malware infection. Also update your computer regularly, especially the antivirus software, web browser and operating system.

Furthermore, please follow your bank's SMS and email alerts with regards to security and data protection and pay attention to SMS and email transaction alerts. Always type out your bank's website, for safety reasons. Do not use your banking password for anything else such as emails or social media etc. Check the information displayed regarding when the last time you logged into your account and make sure it matches. Lastly, periodically review your beneficiaries list and ensure that it matches beneficiaries that you added yourself.

When travelling, we recommend that our customers consider enabling a roaming feature so that you do not miss important notifications from RAKBANK. Also, never use any unsecure Wi-Fi access points.

What can your customers do to ensure they are using a genuine RAKBANK website when they're banking online?

We always advise that our customers type out the bank's website. For safety reasons, never click on links received in emails or messages claiming to be from your bank. Use a secure connection, this is identified with a green area that is visible in the address bar along with https in the URL itself. We also suggest that customers check the domain of the URL as well as the site before providing any details. If you suspect that the site could be fraudulent, do not provide any details and report the site to your bank. For extra precaution, open a new browser window and visit the main page of the site you think you're on, if it looks different, you are then likely to be dealing with a phishing site.

What are the most common forms of online fraud?

- **Phishing/ Vishing/ Smishing** – Do not provide any confidential banking details over phone, messaging apps or SMS malware and ransomware
- **Email Spoofing** – easily avoidable by simply using a reputed email service provider such as Gmail or Outlook
- **Shoulder surfing** – consider banking from any of your devices where no one can see you typing over your shoulder

BUILDING A ROBUST CYBERSECURITY STRATEGY

National Bank of Fujairah has a three pillar approach to protecting customers' information

BY VINCE COOK
CEO OF NATIONAL BANK OF FUJAIRAH

The Covid-19 outbreak has expedited the digitisation movement at an unprecedented pace, and we have witnessed a massive shift from the physical world to the online space. The banking sector, which has been a pioneer in this transformation, is no exception. And while digital banking offers customers convenience and faster processing of financial transactions, it heightens vulnerabilities that banks spend years pre-empting and preparing for.

At National Bank of Fujairah (NBF), we have built a robust cybersecurity strategy that focuses on three main pillars: identity protection, data protection and culture. To protect the identity of our customers, we have deployed the most advanced authentication methods such as biometrics and facial recognition and will continue to evolve our techniques to maximise security. Our approach to data protection is steered by a cross-functional data governance forum, which is designed to ensure we manage data security, privacy, quality and overall performance in an effective way.

We have made relentless efforts to foster a culture whereby employees, partners and customers are fully aware and equipped to deal with potential cybersecurity threats. As part of bank's cyber resiliency programme, we conduct various types of cyberattack simulations like the Red Team exercise, Tabletop Cyber Attack Simulations, Phishing simulations, among others to measure our cyber resiliency capabilities with the help of specialists. We use the learnings from these simulations to improve our cyber resiliency as well as inform and evolve the bank's cybersecurity strategy. We also have specific KPI's for some of these simulations and we can proudly say that for the phishing simulations we have observed a significant improvement in the user's culture change towards cybersecurity.

Looking ahead, we will focus our efforts on strengthening our three cybersecurity pillars by frequently updating our proactive and reactive security controls and overseeing digital channel fraud management to safeguard new the technologies that continue to evolve.

اتحاد مصارف الإمارات
UAE BANKS FEDERATION

شرطة أبوظبي
ABU DHABI POLICE

DUBAI POLICE

TDRA
هيئة تنظيم الاتصالات والحكومة الرقمية
TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

ABCD
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod.
Lorem ipsum dolor sit amet
Your OTP 548796
Lorem ipsum dolor sit amet
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod.
Aa

FRAUDSTERS COULD BE TARGETING YOU.

TOGETHER AGAINST FRAUD

Social Engineering

Do not get tricked into sharing sensitive and personal information over social media.

Stop

- Responding to strangers online asking you to share OTP
- Clicking on pop-up banners claiming your computer is infected
- Entertaining friendly callers from getting your personal information by gaining your trust
- Acting upon mails of messages that create urgency to take action

Think

- Could this be genuine?
- Is it safe to share personal information with a stranger?
- Will your bank call to ask for your personal information?

Protect

- Do not share your OTP or personal information
- Limit the information you share on any digital channel
- Create strong and complex passwords and change them frequently
- Do not download or install suspicious apps
- If you suspect that your personal details have been compromised, report it immediately to your bank

Please report fraud to your bank, in addition, please report on www.uaebf.ae/en/fight-fraud

Disclaimer: Please make sure that you report fraudulent activity to both your bank and UBF.