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

شرطة أبوظبي
ABU DHABI POLICE

DUBAI POLICE

اتحاد مصارف الإمارات
UAE BANKS FEDERATION

FIGHT FRAUD

UAE TOGETHER AGAINST FRAUD

A GULF NEWS SPONSORED SUPPLEMENT
Tuesday, October 20, 2020

THE COVID EFFECT

With the increase in online activity during the pandemic, cybercriminals are finding new and innovative ways to target customers

PAGE 2

SHUTTERSTOCK

THE COVID EFFECT

BY KEITH J FERNANDEZ
SPECIAL TO GN FOCUS

In August, Hozefa Arsiwala was having a late lunch with his wife and daughter during a staycation when an SMS came in. It confirmed that he had just spent Dh50 to buy a T-shirt online. Except that the Sharjah resident hadn't. He immediately rang his bank, one of the largest in the UAE, and learnt the purchase had gone through. A quick Google search told him the store was located in the US.

The same card was also being charged an additional Amazon Prime payment for the preceding three months, something Arsiwala was pursuing with the technology services provider. "The bank offered to open a complaint to pursue the matter and uncover more details about both incidents, but given the time and potential costs involved, it wasn't worth the trouble," he says.

Arsiwala doesn't know if he'd been phished, that is, tricked into revealing sensitive personal data, or if his data had been stolen in a cyberleak, but he was certainly a victim of credit-card fraud, one of many different kinds of online bank hoaxes being reported in the UAE.

Earlier this year, the Central Bank of the UAE warned of a spike in cybercrime and bank fraud, as fraudsters capitalise on the coronavirus pandemic to find new ways to target consumers. The bank rolled out its first national fraud awareness campaign in April, which aims to arm consumers with the skills to protect themselves against scams.

"During times of heightened disruption, there is often a general escalation in cybercriminals' activity," says Anoop Das, cybersecurity expert at the cloud services provider Mimecast Middle East. "There has been a spike in cybercrime across the board and crime for financial gain has been among the most significant. Criminals know that many people are struggling financially and are looking for ways to prey on their desperation."

He offers a chilling example from a recent Mimecast investigation. The log-in page of a major UAE bank had been cloned, with the fake website live since July. Customers had potentially been affected for several months. "If a banking customer were to click on a phishing link, they would be sent to the malicious fraudulent website," he says. "This log-in page is then used to harvest the credentials of the customer, as they are prompted to fill in their information, including their password. Criminals can then use this information to access the user's bank account."

> "Cybercriminals particularly target banking customers and supply chain partners so those connections and credentials must be controlled and monitored."
>
> **AMMAR ENAYA,** REGIONAL DIRECTOR MIDDLE EAST AT VECTRA

Rise in attacks

The company's Threat Intelligence Centre picked up 115,000 Covid-19-related registered spoof domains in the first three months of the pandemic. These offered fake or non-existent goods such as protective masks or Covid-19 cures, or targeted individuals seeking compensation for holidays booked. "The general fear and uncertainty of this year has offered criminals the perfect opportunity to exploit vulnerable people," Das says. "Our researchers saw a massive 751 per cent increase in unsafe clicks during the first three months of the year in the Middle East and North Africa– many of which were likely used for financial gain."

Scamsters have capitalised on the pandemic with creative attack campaigns that play to the present mood. With people's health, jobs and finances all under threat, cyber monitors report an increase in e-mails enticing users to click on unsafe links, purportedly offering information on rising local case numbers, advice on safety measures, tips for claiming stimulus cheques, as well as alerts on coronavirus-linked investment opportunities or relief donations.

ANOOP DAS, Cybersecurity expert, Mimecast Middle East

AMMAR ENAYA Regional Director Middle East, Vectra

ADAM PALMER, Chief Cybersecurity Strategist, Tenable

Focused attacks

"Ransomware, privileged access abuse, data loss and poorly configured services that create vulnerabilities are significant risks," says Ammar Enaya, Regional Director – Middle East at Vectra, an artificial intelligence-based threat detection platform that counts UAE banks among its clients. "Cybercriminals particularly target banking customers and supply chain partners so those connections and credentials must be controlled and monitored too. Banks are also a target for politically motivated attacks seeking to disrupt and destabilise a region's infrastructure. For customers using banking digital services, their credentials will be a prized target for attackers. Banks need to ensure robust access and identity technical controls and also focus on customer security awareness education."

Organisations — including banks — have also been unprepared to have their entire workforce operating remotely. The sudden shift to working from home opened up security gaps for hackers. This week, backup software solutions company Acronis revealed the results of a global survey of 3,400 companies: 39 per cent of companies experienced a videoconferencing attack in the past three months. Malware attacks such as ransomware also have increased during the pandemic, with 31 per cent of companies reporting daily cyberattacks and 50 per cent being targeted at least once a week.

"The attack surface is being expanded by remote work and unsecured personal devices used by employees, increasing the risk to the business," says Adam Palmer, Chief Cybersecurity Strategist at Tenable, a global IT company that tracks cyber exposure. He tells *GN Focus* that traditional risk management is failing, and organisations should integrate their security into one central identity and access management solution, while using privileged access management to restrict access to critical systems and data, to limit the ability for attackers to reach critical systems. "It's important to make sure remote workers' devices are fully configured with endpoint protection and detection. Far too many people, including the most tech-savvy, ignore system updates and patches."

To access the first official page in the UAE for bank customers to report bank fraud, please visit: **www.uaebf.ae/en/fight-fraud**

BE FRAUD SMART AND PROTECT YOUR BANK ACCOUNTS.

Fraudsters trick victims to disclose their personal or financial information. Never disclose such information to anyone. At Citi, we are committed to help you counter fraud with measures such as:

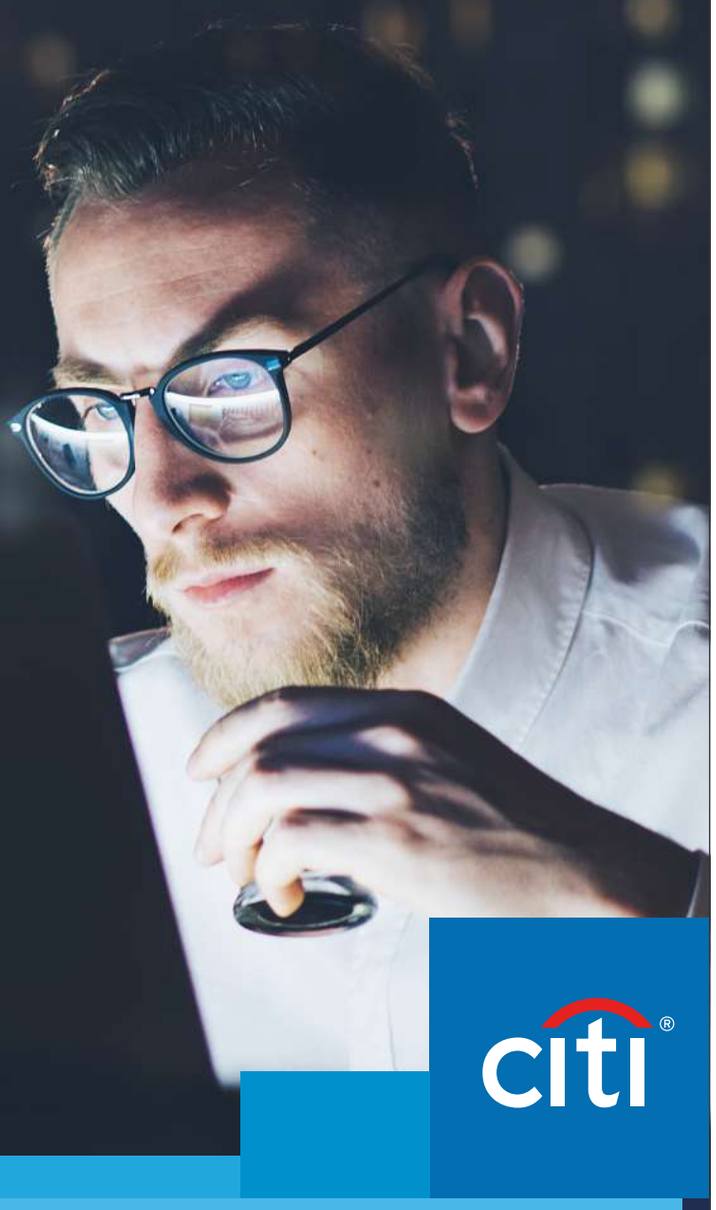
Citi Mobile® Token
generates authentication code on Citi Mobile® App replacing OTPs via SMS.

Fraud Early warnings
unusual activity on credit cards and accounts is immediately reported via SMS, email or phone call.

Citi Alerts
banking and investment notifications.

3D Secure
enhanced security on credit and debit cards.

For more information on keeping your finances safe, visit **www.citibank.ae** and click the security tab at the bottom.



BEST DIGITAL BANK AWARD 2019
GLOBAL FINANCE

BEST CONSUMER INFORMATION SECURITY AND FRAUD MANAGEMENT, UAE AND BAHRAIN.

citi®

Citi will never ask for your personal details.

Never provide the One-Time PIN that is sent to your mobile phone to anyone.

Always check SMS and email alerts from Citibank relating to your account and report any unauthorised transaction to Citibank immediately.

Citibank Terms and Conditions apply, are subject to change and are available upon request. For the current Terms and Conditions, please visit our website www.citibank.ae. Partner terms and conditions also apply. Citibank N. A. makes no warranties and assumes no liability or responsibility with respect to the product and services provided by partner(s) / other entity(ies).

SIM swap fraud drops

Jamal Saleh, Director General of UBF, highlights the success the nation-wide initiative

SIM swap fraud targeting banking customers in the UAE has dramatically declined after launching a major nationwide awareness campaign, a senior banking industry official told Emirates News Agency (WAM).

"SIM swap fraud, the worst among online banking frauds, used to be reported in hundreds in the past. But only one case was reported in recent months since we started the campaign in April with the Central Bank of the UAE, Abu Dhabi Police and Dubai Police," said Jamal Saleh, Director General of UAE Banks Federation (UBF).

"And this is despite the number of online banking fraud attempts having doubled since the start of coronavirus outbreak, as people started spending more time at home and transacting online," he added.

Identity theft

SIM swap fraud is a type of identity theft, where a fraudster manages to get a replacement SIM card of a victim's registered mobile number, using fake identity documents to access online banking services of the victim to steal money.

"The awareness campaign and the strict preventive measures taken by the Telecommunications Regulatory Authority, Etisalat, and du have almost stopped this type of fraud. For example, unlike in the past, the customer has now to go in person with his/her original Emirates ID and fingerprint to request a replacement SIM card," Saleh explained.

Campaign success

The #TogetherAgainstFraud awareness campaign was well received by people across the UAE, and awareness posts on social media platforms secured more than half a million likes and shares, Saleh said.

After SIM swap, magic pen fraud is the other scam that witnessed a decline as very few cases were reported after launching UBF's campaign, he revealed.

Social engineering attempts, through phone calls, text and emails, still constitute the highest number of fraud attempts, but success rate and impact are low compared to other scams such as SIM swap and magic ink.

– WAM

NATIONAL CAMPAIGN BOLSTERS UAE'S READINESS TO FIGHT CYBERCRIME

#TogetherAgainstFraud will run until the end of the year and cover different types of fraud, including Covid-19 related scams

With hundreds of millions of people mandated to stay at home globally to limit the spread of the coronavirus, Covid-19 related fraud is expected to climb as fraudsters exploit people's fear and anxiety during these difficult times. Common scams include targeting victims via email, SMS, phone and social media, with fraudsters posing as genuine organisations, including government entities, banks, and healthcare providers, to trick victims into disclosing personal or financial information.

To counter this, UAE Banks Federation (UBF), the Central Bank of the UAE, Abu Dhabi Police, and Dubai Police launched the UAE's first national fraud awareness campaign in April, which will run until the end of the year. Under the theme #TogetherAgainstFraud, the joint initiative aims to educate and protect consumers from financial cybercrime and fraud, particularly in light of the increased use of digital banking services during the Covid-19 pandemic.

"The banking sector's digital transformation and widespread implementation of online solutions has increased both the complexity and magnitude of financial fraud and cybercrime across the globe," says AbdulAziz Al Ghurair, Chairman of UAE Banks Federation.

"This is a serious threat to society that must be addressed, particularly under these challenging circumstances where fraudsters have become increasingly sophisticated taking advantage of the fear and uncertainty created by the outbreak of the pandemic.

"With the launch of this joint campaign we not only aim to equip the public with the knowledge and resources they need to protect themselves from fraud, but also disrupt the criminal networks that are targeting UAE residents. This can only be achieved if we work together, and on behalf of UBF, I would like to thank the Central Bank of the UAE, Abu Dhabi Police, Dubai Police and our member banks for their continued support and collaboration. By better preparing banks and customers for the future, we are securing a better future for the entire nation.

"Since one of UAE Banks Federation's strategic goals is to reduce fraud across the country, this initiative underpins our will and readiness to tackle fraud and cybercrime, and strengthen our collaborative efforts alongside our partners to combat this threat to society, adopting best practices to safeguard customers against fraud, and focusing on different topics every month," says Al Ghurair.

ABDULAZIZ AL GHURAIR, CHAIRMAN OF UAE BANKS FEDERATION

> "The fight against fraud can only be won if we work together."
>
> **ABDULAZIZ AL GHURAIR**
> CHAIRMAN OF UAE BANKS FEDERATION

"The fight against fraud can only be won if we work together, and since the beginning of the #TogetherAgainstFraud campaign, we have significantly reduced the number of some types of fraud cases across the country with the support of the Central Bank of the UAE and our partners. By better preparing banks and customers for the future, we are securing a better future for the entire nation," adds Al Ghurair.


KEEPING
YOU AND YOUR
LOVED ONES
SAFE, TOGETHER.
Please remain informed, vigilant
and alert when using your cards
and account online.
#FABStaySecure
Visit bankfab.com and find out more.
Grow
Stronger
بنـك أبـوظبـي الأول
FAB
First Abu Dhabi Bank

AI and machine learning can turn the tide

The combined fraud-fighting benefits of these systems are coming to the fore

SHUTTERSTOCK

Most banks rely on teams of human analysts to examine transactions for potential financial crime, but these teams encounter numerous issues. Forty-five per cent of banks say their investigations take too long to complete, and 40 per cent say the investigations result in a high number of false positives, which occur when legitimate transactions that have been mistakenly flagged as fraudulent. Banks can even have false positive rates of more than 90 per cent, resulting in unpleasant experiences for customers as they are forced to resubmit their transactions.

The pros of AI

Financial institutions are exploring many avenues to overcome these stumbling blocks, but few are as promising as artificial intelligence (AI) and machine learning (ML). Here are the fraud-fighting benefits of these systems, as well as the challenges that many banks face in implementing them.

Detection systems driven by AI offer a number of fraud prevention benefits, as they can analyse transactions holistically, comparing each data point within a transaction to every other data point in fractions of a second.

These systems can also compare each transaction against every other transaction banks have ever processed to determine its likelihood of being fraudulent based on variables a human analyst might never notice, such as attempts to log in to the same account with different usernames and passwords over the course of several months or uncharacteristically large transactions.

Banks are deploying AI-based systems in record numbers, with more than $217 billion spent on AI applications for middle-office use cases like fraud prevention and risk assessment.

These investments are paying off, according to fraud prevention specialists, as 80 per cent of experts say AI reduces payments fraud and 63.6 per cent of financial institutions cite AI as a valuable tool for halting fraud before it succeeds.

These systems are commonplace at large banks that have more than $100 billion in assets – 72.7 per cent of which leverage AI – but only 5.5 per cent of all financial institutions reportedly have an AI-based system in place.

The cons

The most obvious explanation for this gap is AI systems' expense, but there are a number of other concerns that keep banks from jumping aboard the AI bandwagon. AI systems often do not operate in real time, with 45.6 per cent of fraud specialists citing this as a concern – a significant obstacle for pay-ments that need to be processed instantly. A lack of transparency is a problem as well, according to 42.8 per cent of specialists. A human analyst could definitely provide justification for rejection of any given transaction, as opposed to many AI systems, whose reasonings may much more nebulous.

Machine learning

Some of these concerns can be addressed by ML, a more advanced form of AI. ML systems take past transactions into account and apply these rules to future analyses to detect financial crime, making them gradually more adept at fighting fraud over time.

Financial crime attempts against banks will likely never cease completely, but the addition of AI and ML to the' fraud-fighting arsenal of financial institutions could go a long way toward making these attempts less likely to succeed.

KEY NUMBERS

Banks are deploying AI-based systems in record numbers, with more than

$217 billion

spent on AI applications

****

About

80%

of experts say AI reduces payments fraud and 63.6 per cent of financial institutions cite AI as a valuable tool for stopping fraud before it succeeds

This article first appeared in the Preventing Financial Crimes Playbook in August by PYMNTS.com, the business-to-business platform for the payments industry

حماية HIMAY

كـــن يقظـــا ..كن حـــريصـــا
Be Security Smart, Stay Vigilant!

مصرف أبوظبي الإسلامي
ADIB

Share a smile, share kindness.

But not your password, no matter what!

Your password is the first line of defense against potential fraudsters. Never share it with anyone under any circumstances. Be vigilant when you shop online or making payments at public places, ensure you are not accidentally revealing your password to anybody.

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

Change your Passwords and PINs regularly

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

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

STOP IDENTITY THEFT

Here're some steps to safeguard against fraudsters

GN FOCUS REPORT

The pandemic has accelerated the UAE's transition to a cashless society. Almost two-thirds of people in the UAE, or 64 per cent, expect the country to become fully cashless by 2030, a poll by Standard Chartered found in September.

The survey, which was conducted globally among 12,000 respondents aged 18 and above, also found that 73 per cent of the UAE's respondents believe Covid-19 has made them more positive about online shopping. Here are a few simple steps that shoppers can take to avoid financial fraud:

Have a secure log-in

Use a different password for each of your online shopping accounts so that if someone grabs your username and password for one website, they won't be able to go on a shopping spree on other accounts as well. Some banks in the UAE have also introduced multifactor authentication, which requires users to enter a code that is sent to the registered phone number when they try to log on. The added step can make it harder for thieves with stolen user names and passwords to take over people's accounts. Shoppers can ask retailers to remember certain devices, such as their phones and home computers, but require the codes whenever someone tries to log on from a new device.

Transaction alerts

All banks in the UAE allow customers to sign up for alerts directly via email, text message or the mobile banking app. The feature allows cardholders to get alerts for transactions in real time and immediately identify potentially fraudulent activity. With visibility and control over their accounts, consumers can take immediate action to protect themselves from security threats and fraud.

Payment devices

New mobile payment options such as Apple Pay and Android Pay let consumers shop with their smartphones. Instead of swiping or inserting their credit cards, shoppers tap their phones, which transmit a unique code to the retailer for each purchase. This is useless to fraudsters and in the case of Apple Pay, shoppers have an added protection by requiring that their finger prints be used to complete the transaction.

Monitor transactions

Most banks will refund consumers for fraudulent charges made with their debit or credit cards as long as they report it in a timely matter. Consumers should check their transactions every day or every other day to scan for unauthorised purchases, especially when they are using their credit cards frequently. If you don't have time to monitor transactions daily, then you can set up alerts to have a message sent to your phone or email every time your card is used.

Stick to one card

Using one card for most of your purchases can limit the number of cards you need to track closely. It also cuts down the chances that more than one card will be compromised, though you should still check transactions on all of your cards periodically. Try to use a card that is different from the one you use to pay your monthly bills. That way you can avoid having to reset all of your payment settings if your card is stolen.

Device identification

What this does is it evaluates the unique ID of the device (smartphone, laptop or tablet) used to make a digital transaction to help identify suspicious activity. Security experts advocate sticking to trusted devices — ones that belong to you and under your control — for any kind of online transactions.

Watch out for scams

Fraudsters often send emails that promise consumers a phony promotion if they enter their personal information or click a link. The messages can include logos that closely resemble those of the legitimate retailers. And the links may download malware on to your computer, giving thieves access to your personal information. Shoppers should ensure that they check the web address included in the messages and also avoid clicking on links. Look for https in any URL.

SHUTTERSTOCK

البنك العربي المتحد
UNITED ARAB BANK

Triple Your Cashback

Apply for UAB Credit Card today and triple your Cashback on all your spends! Offer eligible from 1st of October 2020 to 31st of December 2020.

Terms and conditions apply

@uabuae | uab.ae | 800 474

8 TYPES OF FRAUD TO WATCH OUT FOR IN THE UAE

Technology and social engineering tactics have seen fraudsters implement a number of techniques to separate you from your money. Here's how they work

BY RIAZ NAQVI
SPECIAL TO GN FOCUS

Earlier this year, the UAE Banks Federation (UBF), Central Bank of the UAE (CBUAE), and Abu Dhabi and Dubai Police joined forces to launch the country's first large-scale national fraud awareness campaign. The initiative was rolled out during the UAE National Sterlisation Programme, with larger numbers of residents turning to digital banking as they stayed home to help flatten the coronavirus curve. The ongoing awareness campaign's primary aim is to educate consumers about the UAE's most common cybercrime and fraud techniques.

"The fraud awareness campaign, underscored by a series of interactive and educational materials, is aimed at informing consumers about the proliferation of phishing activities while enabling them to stay alert," said Abdulhamid Saeed, Governor of the CBUAE, in the press release announcing the news.

Here GN Focus profiles eight types of fraud you need to watch out for in the UAE.

1. EMAIL

What is it? An email, purportedly from the UAE Central Bank, with an alarming message: Your debit card and bank account are now frozen due to "security reasons". It also contains an urgent call to action, pushing the reader to dial a mobile number within 24 hours to reactivate their account. The person picking up will ask for details of your account for "verification purposes". Alternatively, there may be a link present that takes you to a form, where you are asked to type the information in. The mail, which may include the Central Bank's logo, may have these contents in an attached PDF.

Tip Call your bank using one of the registered numbers on its official website. They will be able to tell you if your account or card has been frozen.

2. LOTTERY

What is it? This usually takes the form of an image sent from an unregistered number via WhatsApp. There will be a large logo at the top, typically of a hypermarket or major UAE retailer, followed by a message informing you that you have won a large cash prize. The message will then direct you to contact a mobile number and share personal finance details such as your account number. Two years ago, fraudulent messages bearing the logo of LuLu hypermarket were so prevalent that the retailer took out ads in national newspapers warning residents about the scam.

Tip Mark the message as spam and delete.

3. ATMS

What is it? Thieves employ a number of devious tricks at ATMs. They may strategically place a tiny camera facing the machine's keypad in a bid to record your hand typing in your PIN. Another technique sees the thief place a false keypad, which records your PIN, on top of the real thing. Once you've concluded your business at the machine, the false keypad is removed. Finally, fraudsters may attach a device on top of an ATM's card slot. When you put your card in, it scans both sides of your card to memory, giving the scammer the number, expiry date and three-digit security code.

Tip Before putting your card in, take a close look at the ATM on your next visit. Is the keypad fixed into the machine and easy to hide with one hand? Is there a removable object around the card slot? Always be aware of your surroundings.

4. SIM SWAP

What is it? This technique works using mobile phone-based authentication, a process your bank uses when you want to pay for something online from a previously unused website or app. After you've input your payment details and hit order, the bank will SMS a one-time password (OTP) to your registered mobile number. SIM swappers try to play the system by contacting the victim's mobile service provider and, using personal information gleaned from social media and other sources, impersonates the victim by answering security questions. The fraudster reports the phone as lost and requests activation of a new SIM card, which is in the fraudster's possession. Then, using your email address, they will request a new password through OTP, which then gives them access to the account.

Tip If you find your phone suddenly has no coverage, contact your service provider and check what the problem is. Never share the answers to your security questions with a random caller, and read your bank statements regularly.

5. MAGIC INK

What is it? Unlike the other fraud types on this list, magic ink fraud requires a personal touch. After inviting their target out for a coffee in the guise of a banker, the fraudster will present them with pre-filled forms and paperwork for a new credit card or personal loan, as well as a cheque that requires the victim's signature. However, the writing that's already on the cheque is no ordinary ink – it vanishes once the paper is heated to a particular temperature. The scammer now has a blank cheque with the victim's original signature to do with as they please – and with their account details, they know exactly how much they'll be able to withdraw from an account.

Tips Always request a proper look at a financial representative's official ID. Sign and fill out forms using your own pen. Contact the bank prior to your appointment to verify the person.

6. FUND TRANSFER

What is it? In a bustling trading hub such as the UAE, businesses tend to deal with suppliers and clients from all over the world, primarily via email. It's important to heed caution before clicking links in suspicious mails, as malware may be surreptitiously downloaded to your PC or smartphone. This may give hackers access to your screen and keystrokes, which they can then use to find out supplier information and create impostor accounts. The fake account will get in touch with the victim and ask them to send payments to a new bank or number.

Tip Look carefully at the email address when you receive a mail requesting a new payment avenue. Is it slightly different? If not, get in touch with the person to check whether they have indeed asked you to change the means of payment – it could be that their email has been hacked and they are unaware of the message.

7. PHONE FRAUD

What is it? Also known as voice phishing, or vishing, this happens when you get a call from a person claiming to be employed by your bank. They will ask some personal information under the cover of security questions to try and glean responses to your account's security questions. They may tell you that an Emirates ID or debit/credit card has been temporarily blocked. Alternatively, you may receive an automated robocall requesting that you type in details such as card number, expiry date and security code.

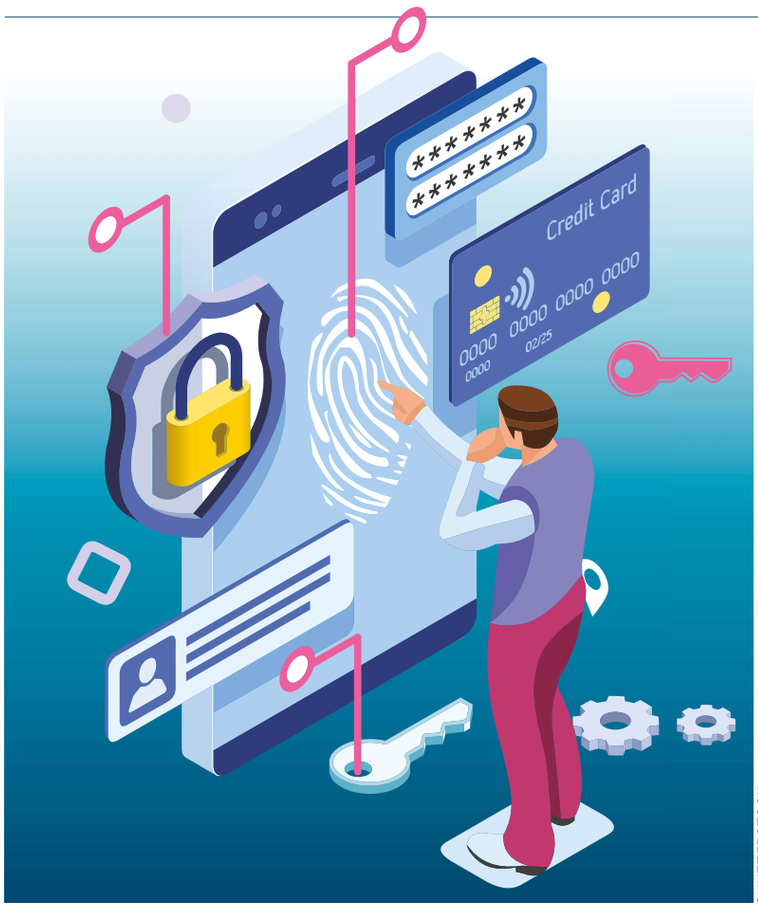
Tip Don't tell them anything. Hang up, and get in touch with your bank via its official call centre to check whether any cards or accounts have indeed been frozen.

8. DATA PRIVACY

What is it? A breach of personal information such as your Emirates ID number, passport details, mother's birthday or maiden name, and sensitive data such as debit/credit card numbers, ATM PIN or your bank account details.

Tips Review the personal details you have shared on social media platforms – including ones you barely use – and remove phone numbers and dates of birth; periodically change your passwords, ensuring they are strong and complex; avoid using public Wi-Fi for accessing digital banking or other sensitive data; use an antivirus software on your PC; avoid downloading apps from unknown or unverified sources; and ensure your phone has the latest security updates.

SHUTTERSTOCK



SHUTTERSTOCK

12 TIPS TO KEEP YOUR TRANSACTIONS SECURE

Practical, simple dos and don'ts for a safe banking experience

BY AYMAN ALQUDSI
SPECIAL TO GN FOCUS

1 Be alert

Be alert to the fact that scams exist. When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in-person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is.

2 Do your research

Know who you're dealing with. If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. Do a Google image search on photos or search the internet for others who may have had dealings with them. If a message or email comes from a friend and it seems unusual or out of character for them, contact your friend directly to check that it was really them who sent it.

3 Avoid suspicious texts

Do not open suspicious texts, pop-up windows or click-on links or attachments in emails – delete them: If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.

4 Remote access

Don't respond to phone calls about your computer asking for remote access – hang up even if they mention a well-known company. Scammers will often ask you to turn on your computer to fix a problem or install a free upgrade, which is actually a virus that will give them your passwords and personal details.

5 Lock mailbox

Keep your personal details secure. Put a lock on your mailbox and shred your bills and other important documents before throwing them out.

6 Keep passwords safe

Keep your passwords and PIN numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

7 Safeguard devices

Keep your mobile devices and computers secure. Always use password protection, don't share access with others (including remotely), keep updating security software and backing up content. Install mobile security software and keep it up to date. Don't forget to install updates for your device operating system and banking app too as they become available.

8 WiFi safety

Protect your WiFi network with a password and avoid using public computers or Wi-Fi hotspots to access online banking or provide personal information. Don't carry out sensitive financial transactions using public Wi-Fi or unknown public networks, which makes you vulnerable – you never know who may be poking around and watching what you're doing online.

9 Update passwords

Choose your passwords carefully. Use passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper- and lower-case letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.

10 Review privacy

Review your privacy and security settings on social media. If you use social networking sites, such as Facebook, be careful who you connect with and learn how to use your privacy and security settings to ensure you stay safe. If you recognise suspicious behaviour, have clicked on spam or have been scammed online, take steps to secure your account and be sure to report it.

11 Beware of requests

Beware of any requests for your details or money. Never send money or give credit-card details, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offence. Be wary of unusual payment requests. Scammers will often ask you to use an unusual payment method, including preloaded debit cards, gift cards, iTunes cards or virtual currency such as bitcoin.

12 Online safety

Be careful when shopping online. Beware of offers that seem too good to be true, and always use an online shopping service that you know and trust. Think twice before using virtual currencies (like bitcoin) – they do not have the same protections as other transaction methods, which means you can't get your money back once you send it.

The writer is the Chief Information Officer at UAB

VIGILANCE IS ALL YOU NEED TO DEFEAT CYBER THREAT

Stay Alert!

As the world comes together to fight Covid-19, cybercriminals have also come together to perpetuate their internet scams against unaware victims.

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

As banking connects you across devices, platforms, and channels, National Bank of Fujairah has initiated various digital security features to mitigate fraud, including the most advanced multi-factor authentication systems, such as biometrics and facial recognition and will continue to maximise security to safeguard the technological advancement that continues to evolve addressing your growing banking needs.

Call 8008**NBF**(623)

nbf.ae

nbf
In good hands

THE FUTURE OF PAYMENTS

As the Internet of Things (IoT) evolves, payments will fit into everything from smart fashion to smart cities

GN FOCUS REPORT

WEARABLES

Right now: Having initially focused on fitness and health, next-generation wearables such as the Fitbit Ionic and Garmin vivoactive 3 smartwatches are making life on the go simpler than ever with easy and more secure contactless payments thanks to digital tokenisation technology.

What's next: Welcome to the world of smart fashion. Clothing will be packed with technology, making what you wear functional and comfortable, while reducing the burden of multiple devices. Payment technologies will incorporate into clothes, enabling you to communicate, plan and pay without having to reach for your wallet or phone. Built-in batteries will be thin, flexible and efficient, minimising or perhaps even forgoing the need to recharge.

TRANSPORT

Right now: Autonomous and connected cars are already here. Visa and Honda revealed a proof of concept connected car that makes paying for things such as gas and parking easy. Drivers no longer need to rummage through their wallets to pay; instead they pay via two in-car apps, which Visa has developed alongside its infrastructure partners.

What's next: When we look ahead to the rise of self-driving autonomous vehicles, we can see how the car will pivot into a roving lounge, freeing consumers from navigation and operation. With the Visa Token Service, a secure platform for mobile transactions, in-car payments will soon be within a driver's reach. Drivers will be able to view and complete purchases to smart parking metres and fuel pumps directly from their car consoles.

HOME

Right now: Homes today already contain devices such as video consoles, voice-activated smart speakers and smart thermostats. Present IoT smart home solutions can even automatically replenish supplies, with Samsung and Trustonic's connected refrigerators able to place orders directly.

What's next: Adoption of smart household devices, especially in more developed markets where connectivity via central internet hubs will facilitate purchases by various household devices. Voice-activated speakers such as Alexa Echo and Google Home will be the most common way for consumers to search for anything online and even contact customer service. A future smart home will remember your preferences and past purchases, whether paying bills, grocery shopping, travel planning or gifting.

RETAIL

Right now: The mobile revolution is enabling more interactions with consumers. Increased security and flexible points of sale mean that the divide between online and in-person is rapidly disappearing. IoT payment technologies have made it easier than ever to help consumers find – and pay for – products, as well as use coupons, points and other rewards.

What's next: IoT will revolutionise retail. As more devices become connected, they become platforms for commerce able to make a payment itself, support a payment to be accepted, or both. Consumers will expect personalised and efficient shopping experiences. Best-in-class retailers will provide product information that's tailored and responsive. Imagine having your food or purchases delivered to your door via drones or robot.

FUTURE CITIES

Right now: Cities worldwide are leveraging internet of things (IoT) to gain insights, cut costs, propel new business models and improve consumer user experiences. IoT is also enabling data-gathering to inform every element of city living, from street lighting to waste management. Visa's Innovation Centre in Dubai is dedicated to working with its partners to accelerate the development of smart cities.

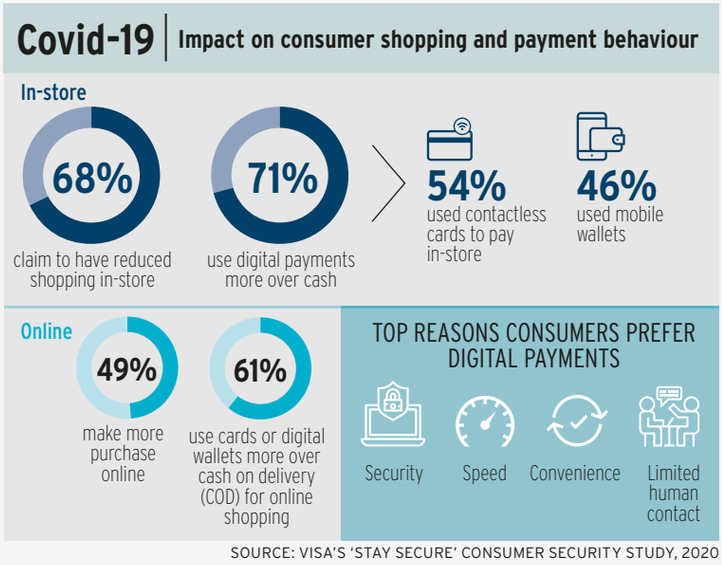
What's next: With more than 20 billion devices expected to come online by the end of 2020, the future smart city is an integrated and responsive world that benefits the environment, people and government. Smart payment technologies can enable more efficient government services, providing convenience for citizens in paying taxes or for public transportation.

– The article was co-created with Visa, the world's leader in digital payments

SHUTTERSTOCK

Cashless to continue after the pandemic

Consumer behaviour changes due to the pandemic, such as buying online and increasing use of digital payments, are likely to continue



SOURCE: VISA'S 'STAY SECURE' CONSUMER SECURITY STUDY, 2020

GN FOCUS REPORT

Consumers in the UAE will continue using contactless payments for shopping at physical stores and making digital payments online even after Covid-19 subsides, signalling that changes spurred by the outbreak are here to stay.

Some 43 per cent of consumers in the UAE will continue using contactless payments more in stores and 48 per cent will increase their use of online payments with cards or digital wallets for future e-commerce purchases, according to a study by Dubai Police, Dubai Economy and Visa earlier this year.

Ahmad Al Zaabi, Director of Consumer Protection in the Commercial Compliance & Consumer Protection (CCCP) sector, Dubai Economy, said: "The study shows that consumer behaviour changes due to the pandemic such as shifting online and increasing use of digital payments are likely to continue even after the pandemic – an important takeaway for businesses developing strategies for the post-Covid-19 consumer and market overall."

Sixty-eight per cent of respondents surveyed in the UAE have reduced shopping in-store since the outbreak of the pandemic and 49 per cent are shopping online more. When they do shop at stores, 71 per cent are using digital payments over cash with the majority using contactless cards (54 per cent) and mobile wallets (46 per cent) more. For consumers shopping more online, the majority (61 per cent) use cards or digital wallets more to pay online over cash on delivery. Increased trust in the security of the payment technology, speed, convenience and limited human contact were the top reasons cited for their increased preference for digital payments.

"The pandemic has changed how consumers shop and pay with increased reliance on and preference for digital commerce," said Neil Fernandes, Visa's Head of Risk for Middle East and North Africa. "With increased usage both among experienced and first-time users, cybercriminals too are keen to capitalise on the increased activity and vulnerability, especially of first-time online shoppers. That is why educating consumers about safe payment behaviour is critical not only for the moment but as we move forward and adapt to the new normal."

Brigadier Jamal Salem Al Jalaf, Director of Criminal Investigation Department in Dubai Police, said: "Fraudsters are seeking to take advantage of people spending more time online, preying on their anxieties, and exploiting new systems of remote working. Government authorities, private sector, and the local community all have an important part to play to ensure we are all protected."

TACKLING THE SURGE IN CYBERCRIME

Customers need to adopt security measures and be aware of the best practices to prevent fraud

BY GEOFF STECYK
CHIEF OPERATING OFFICER, RAKBANK

The new normal has promoted an astounding development of the UAE's digital footprint through work-from-home solutions and a technological shift that enabled businesses to move their operations online.

Driven by the need for digital and cashless payment solutions, RAKBANK is one of the first banks to have undergone a digital transformation that enhanced its banking services. From contactless payments to instant remittances, innovation is aligned with our diversification and cost-optimisation strategy. For us, digital solutions are among the primary focus areas, offering customers secure banking services.

However, one of the downsides of this massive shift to online was the surge in cybercrime rates. The hike in unemployment and online activities attracted cybercriminals who are always quick to take advantage of such situations. A rise in cyber frauds targeting customers through phishing, vishing and SMShing was noted.

Social media chat features and email campaigns impersonating well-known entities such as the World Health Organisation have been used creatively to target customers and get them to click on a link or open an attachment containing malware. Novel methods were adopted to deceive customers including fake websites, lottery scams or transaction frauds such as SIM-swaps. This included sending misleading emails requesting money transfers, including ransomware and crypto-miner attacks on businesses.

Fortunately these ploys can be avoided through adopting security measures such as only using your personal devices (phones, tablets and PCs), routinely updating them and applying patches, investing in a paid antivirus subscription and regularly updating virus definition, being suspicious of emails containing links and attachments that claim to be from their bank or a government body and always navigating to the website by typing the URL in the browser.

We recommend backing up business and personal data regularly to be able to restore it in case of ransomware infection and to regularly monitor bank statements and SMS/email alerts for any suspicious transactions. Furthermore, most websites offer a two-factor-authentication option that we advise enabling. Be wary of public WiFi and protect your home WiFi network with WiFi Protected Access 2 (WPA2) and lastly limit the amount of information you post online as it can be used against you.

10 THINGS TO KEEP IN MIND

- Use different passwords across your bank accounts and other websites.
- Keep your computer and mobile devices updated with latest patches.
- Fraudsters can use many channels such as email, chat, messenger services, SMS& phone calls to ask for your details.
- Most email and social media sites allow the use of two factor authentication, enable this option.
- Invest in a good antivirus solution.
- A password that is easy to remember can also be guessed easily by attackers.
- Secure your home Wi-Fi network and avoid free Wi-Fi services (such as coffee shops) for banking online.
- Report any suspicious activity to your bank or law enforcement.
- Limit the amount of information about yourself that you post on social media sites.
- Back up your important data regularly.

'Banks need to be more agile'

Alexander Thomas, Chief Risk Officer at UAB, tells *GN Focus* why financial institutions need to embrace new approaches to predict and prevent fraud

Is Covid-19 leading to a rise in fraud?

There has been an increase in phishing and smishing (using text messages) scams and identity thefts in the current scenario.

Fraudsters are also exploiting the downturn in interest rates and contacting unsuspecting consumers, offering 'better products', often tricking their victims into transferring money. Moreover, in some scams fraudsters pose as government entities, banks and healthcare providers to trick individuals to reveal their personal and/or financial information.

There has also been a rise in the use of video conferencing facilities, but some of these have been shown to have sub-optimal security standards, with instances of uninvited parties eavesdropping or even hijacking the conversations.

Why is tackling fraud important for the banking sector?

As the banking sector continues to embrace technology, fraudsters are becoming sophisticated and can swiftly adapt approaches to conduct criminal activities, which could result in significant losses for banks.

Technology represents a great opportunity, as well as a responsibility for banks, to cultivate the trust of their customers and manage the expectations of the regulators. Therefore, banks need to be more agile to respond to new threats and embrace new approaches and technologies to predict and prevent fraud.

With employees working from home amid Covid-19, the bank's VPN servers have now become paramount and their security should be the key focus of IT functions. Most home networks lack the same level of security that exists at workplace, and this brings a great responsibility for the banks' IT function to mitigate the cyber risk.

Banks are diligently working on cybersecurity awareness, but customers play a key role in the prevention and detection of fraudulent activity. More efforts are needed to create awareness for customers about fraud and scams.

HOW TO BUILD A ROBUST CYBERSECURITY STRATEGY IN A COVID-19 WORLD

Strengthen layered security controls, beef up cyber-resilient capabilities and educate the workforce as well as customers

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 past few months have similarly accelerated the digital transformation in the banking sector ushering in a new age of banking. At National Bank of Fujairah (NBF), we can proudly report that more than 70 per cent of our customers have successfully transitioned from traditional to online banking and in some processing areas more than 90 per cent of transactions are now fully automated.

While digital banking provides faster processing of financial transactions and more convenience, this new normal has heightened vulnerabilities that banks spend much time and effort to effectively counter. At NBF, our cybersecurity strategy sits at the centre of our digitisation model and we have worked tirelessly towards strengthening our layered security controls, beefing up our cyber-resilient capabilities and educating our workforce and customers on cyberattacks on a regular and ongoing basis.

At 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.

Lastly, 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. We conduct awareness sessions on a regular basis where we educate our staff and customers about cyberattacks and how best to navigate them. As a result, after measuring our staff's readiness to cybersecurity, we can proudly report that their ability to mitigate threats has increased by 90 per cent over the past five years.

In fact, I am very proud of the fact that in one recent phishing simulation we experienced zero hooks and believe that it is from building on such basic awareness we will remain a safe place to do business.

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 technologies that continue to evolve.

Remain vigilant to avoid becoming a victim

It is critical to stay educated and be aware of risks as well as comply with prevention strategies and authentication policies

SHUTTERSTOCK

Over the past few years, the UAE's financial market has embraced many new digital development strategies. However, given the coronavirus pandemic in 2020, this shift from analogue to digital has seen an exponential shift. Now, consumers have greater access to their financial institutions and ability to smoothly access their finances anywhere among a plethora of devices. Therefore, it is immensely critical to stay educated and aware of fraud risks, comply with prevention strategies, authentication policies and remain vigilant about our own role in not becoming a victim of fraud.

In the case of social engineering scams, fraudsters target unsuspecting customers, through SMS and emails, soliciting personal information related to their bank accounts, including SMS OTPs. Once provided by the customer, fraudsters are able to potentially take over accounts and steal money by transferring it out.

As a means of prevention, Citi regularly runs client education drives and spreads awareness along with tips and tools. Its latest offering is the Citi Mobile Token, which allows the customer to generate an authentication code without depending on SMS OTPs. Another means by which Citi is improving risk prevention is in using biometric authentication for card deliveries.

Citi continues to invest heavily in the latest technology within the field of fraud prevention and detection. In fact, *Global Finance* magazine awarded Citibank UAE and Bahrain under the award category of Best Consumer Information Security and Fraud Management for 2019. Citi always places the utmost importance on protecting the safety of its clients' and their data.

PROTECT YOURSELF FROM EVOLVING FRAUD TECHNIQUES

As fraudsters continue to adapt to change in technology, customers need to stay cautious

BY PRADEEP RANA
GROUP CHIEF RISK OFFICER, FIRST ABU DHABI BANK

At First Abu Dhabi Bank (FAB), we take great pride in protecting our customers against fraud, as we strive to put them first in all that we do. Fraud attempts continue to adapt as technology and digital capabilities evolve, and one of the latest trends that we are witnessing at the moment includes fraudsters using social engineering techniques to get victims to share their secured credentials and authentication codes, including One Time Passwords (OTPs).

Here're some tips on how to protect yourself from such schemes:

- **OTP scams:** Fraudsters misuse victim accounts at all levels. They contact individuals impersonating bank representatives or employees from official entities, compelling them to share an OTP message that they received, in order to update their contact details. They sometimes go as far as threatening the victim that their account will get blocked if they do not cooperate. Victims are tricked into sharing their OTP, leading to unauthorised transactions.
- **How to protect yourself:** Ensure the caller introduces themselves along with their designation. Verify that the number they are calling you from is legitimate. Always check the purpose of receiving an OTP, as usually OTP messages include information on the amount and reason for receiving the notification. In any case, never share your OTP with anyone.
- **Business Email Compromise scams:** In this scenario, companies receive an email from a fraudster impersonating a supplier or counterparty requesting them to make an urgent payment to an updated IBAN or account. Based on such instructions, victims send the funds to the fraudster's account (beneficiary).
- **How to protect yourself:** When receiving such emails from your counterparts, immediately contact them on their usual registered telephone number to verify the validity of the email and whether they have in fact updated their account details.
- **Mule accounts:** Fraudsters approach genuine account holders with business or employment offers, which require them to receive payments into their account. After being told that a sum is to be left for them, they are then directed to hand over large amounts of the transaction to fraudsters either in cash or through onward transfers.
- **How to protect yourself:** Never use your bank account for any unrelated third-party transaction. If someone approaches you with offers that are too good to be true, be wary. Do your research, and when in doubt, contact your relationship manager or bank.

TIGHTER SECURITY MEASURES AND CONTROLS IN PLACE

It is perhaps no surprise that cybercrime spiked during the lockdown to tackle Covid-19. Since the beginning of May, phishing attempts have risen 600 per cent in the UAE, while 80 per cent of companies claim to have seen an increase in cyberattacks.

There are numerous contributing factors to the acceleration of cyber fraud. Firstly, phishing attacks had customised messages related to the pandemic. Secondly, working from home and the adoption of various digital platforms encouraged fraudsters to be opportunistic. Thirdly, individuals accessed more data at home giving potential opportunities for misuse by fraudsters. Finally, individuals using open public WiFi, which often has no security measures, was a further invitation for online criminals to strike.

Due to the pandemic, fraud protection has become more

essential than ever, especially to banking customers who are always the number-one target for fraudsters. There has been a 230 per cent rise in attacks on financial institutions attributed to the pandemic, as cybercriminals were quick to adapt well-known schemes by leveraging emotions such as fear and confusion.

In this new reality came new challenges that companies and institutions need to face, such as the enhancement of physical security controls; risk of internal and external fraud; risk of availability and business disruption; and the possibility of data leakage.

As a leading Islamic bank, 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.

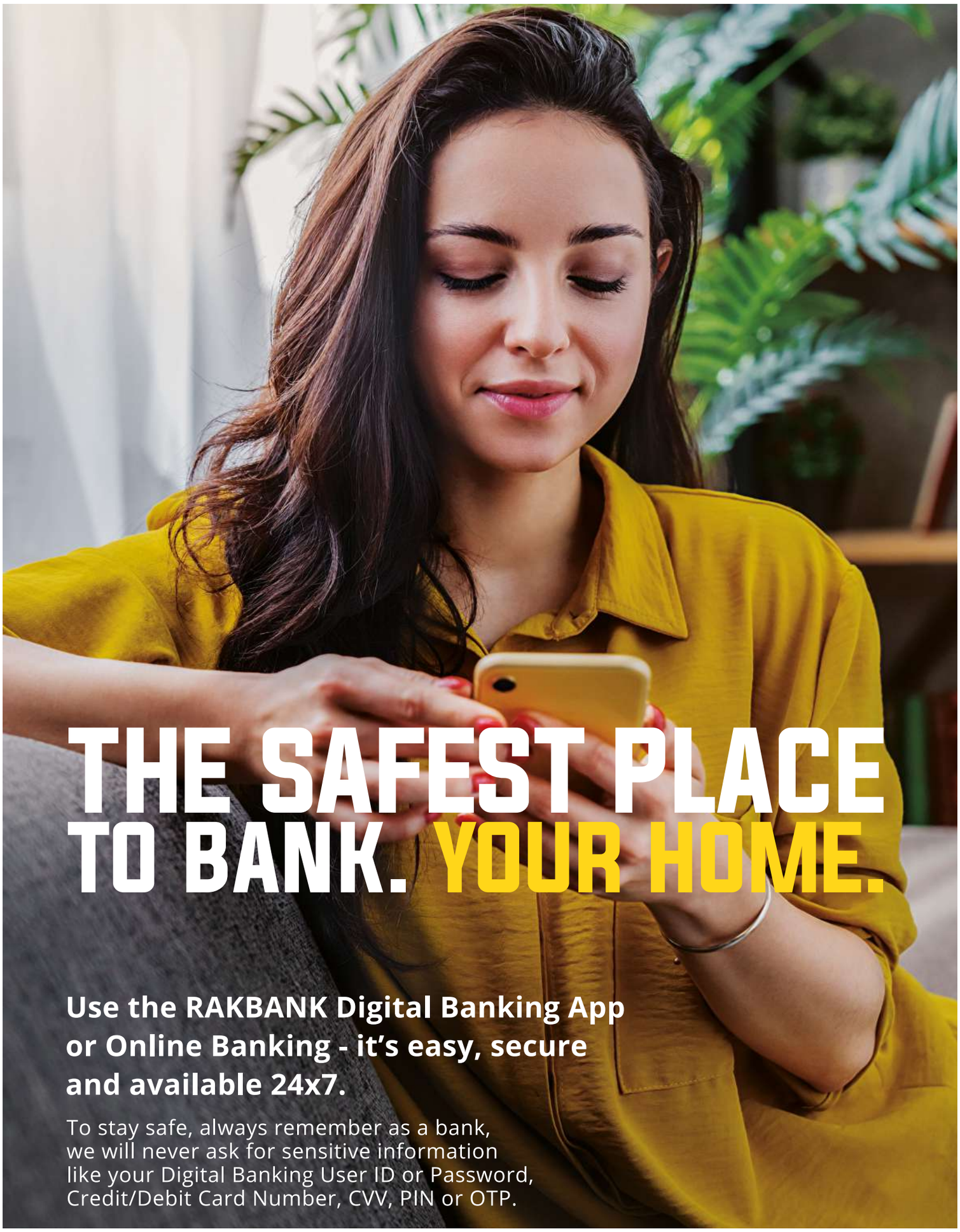
ADIB has introduced a new secure set of collaboration tools to increase business productivity without compromising information security. The bank has also enhanced its technical, procedural and security awareness controls, increased the portfolio of secure remote connectivity services to cater to different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

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 practise secure working, while updating the bank's readiness plan to meet all potential scenarios.

GN FOCUS

A GULF NEWS SPONSORED SUPPLEMENT
SENIOR EDITOR PRIYA MATHEW | **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



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

RAKBANK
Simply Better

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.
شرطة أبوظبي
ABU DHABI POLICE
DUBAI POLICE
اتحاد مصارف الإمارات
UAE BANKS FEDERATION

FRAUDSTERS COULD BE TARGETING YOU

TOGETHER AGAINST FRAUD

How to stay safe from frauds?

E-Mail Fraud
Never click on any suspicious links

Lottery Fraud
Ignore requests to send money to claim prizes

ATM Fraud
Watch out for suspicious objects or people while at ATM

Sim Swap Fraud
Check with your service provider if there is a sudden cellular network failure

Magic Ink Fraud
Never Issue a blank cheque and always fill in details with your own pen

Fund Transfer Fraud
Check with your clients before you transfer funds to a new account

Data Privacy
Create strong passwords and don't download unknown apps

Phone Fraud
Never share any personal information over the phone

To report fraudulent activities,
visit www.uaebf.ae/en/fight-fraud

FIGHT FRAUD

SUTRA...