Digital Security Insights

Promoting a Safer Digital Environment

Guest Contributor

Kagiso Patrick
Fraud Manager, FNB Botswana

Cyber scams in the era of COVID-19

Botswana like the rest of the world was caught by surprise by the COVID-19 pandemic. The rapid speed at which the coronavirus spreads and the fact that there is yet no vaccine or cure for the disease has meant that the government has had to implement extra ordinary measures to combat it, that include among others, extreme social distancing or lockdown. Fighting the disease also means that government must make emergency purchases of medical equipment and supplies to deal with the disease which is mostly done through local companies. To put this into perspective, this disease has created an increase in global demand for these supplies and it is increasingly becoming obvious that there is a global shortage as well, and this is unfortunately where criminals are taking advantage and stealing from desperate and unsuspecting people, more especially business owners, through a variety of scams.
Business people are unfortunately falling prey to these unscrupulous individuals at a very alarming rate. This situation has therefore created a need for banks to increase their level of preparedness, public engagement and education on these scams and how they can protect themselves.

Supplier Scams
Be cautious about what is known as “supplier scams”. Criminals have reacted fast to take advantage of the commotion and panic brought about by the pandemic by creating fake online shops, websites and social media accounts pretending to be selling medical equipment and supplies. Now, out of desperation and in order to beat the competition, most people fail to conduct the necessary due diligence on suppliers and end up doing business with people they do not have sufficient background information on. They end up paying for goods that are non-existent from non-existent suppliers.

Phishing, Vashing and Smashing Scams
Phishing, vishing and smashing scams are also on the increase. Similarly, because most people are locked up in their homes with limited or restricted movement, they have resorted to spending more time on the internet which makes them easy targets for cyber criminals.
Perpetrators often send out phishing or spoofed emails imitating reputable organisations like the WHO or government entities like the Ministry of Health or BURS offering relief services to people affected by the COVID-19 pandemic.
Usually, they would ask a user to click on a link in the email or ask them to download an attachment. These links or attachments are usually infected with viruses or ransomware which infect your computer or smartphone making it easy for criminals to steal your personal information. Also, criminals may use phishing sites disguised as a trustworthy entity and make contact with potential victims via email, phone calls “vishing” or text messages “SMishing” with the intention to trick them in to disclosing their passwords, usernames, account details or credit card details for malicious purposes. It is therefore advisable to exercise caution and avoid clicking links or downloading attachments from unsolicited emails or messages in the event you receive such emails. Open a new browser to access the official site of that entity to verify the information or/and avoid using contacts which come with the email.(.....Continued to Page 2)

Presented by: eBotho for a better e-society

Supported by: Universal Access and Service Fund; Botswana Communications Regulatory Authority

Secondly, I want to discuss what we call business email compromise or change in banking details scam. Criminals have been able to divert payments to suppliers by sending bogus notifications for change-in-banking details to customers seeking to make payments. Usually, criminals create and use an email address similar to that of the supplier to send these bogus instructions. These are often very difficult to detect so treat every such instruction with suspicion and desist from replying directly to such emails. Rather reply to previous emails to verify the instruction or alternatively directly call a known contact.

During this time of COVID-19 and of course any other time, be cautious against sharing your banking details on unverified websites, particularly on promotional websites where you are told that you have won something or offered cheap holidays deals.

Doing so leaves your bank accounts vulnerable and to date many customers have lost money through subscriptions on dubious websites. One must use reputable online payment systems or platforms like PayPal. Furthermore, be cautious against sharing your personal, credit card or online banking details over the phone unless you have personally made the call using a number from a trusted source.

ATM Card swopping

Now, as lockdown restrictions are starting to ease, we may eventually see borders opening for movement across the borders more especially between Botswana and South Africa. South Africa is currently proving to be a hot spot for criminal activities targeting Botswana travellers. A lot of people have fallen victim to a variety of criminal activities in that country, where commonly targeted people are those using ATMs to withdraw cash. Card swopping which happens when criminals temper with the functionality of an ATM and then offer to help unsuspecting users to use the machine is becoming prevalent. In the process of "helping", the criminals insist on taking control of the user's card and then distract their attention with something whilst they swap the card with a different but similar looking card. Oblivious of these, the customer then either leaves the ATM dejected that they could not transact or continue making attempts to withdraw cash until the card they are using gets retained by the ATM because they would have invariably made many attempts using a wrong pin for the card (remember that the criminal would have left with the owner's card). It doesn't usually take long before the criminals start using the card to either withdrawn money at a nearby ATM or swipe goods at a nearby merchant.

Time is of great essence to the criminals and they always want to access your money before you can call your bank and block the card, and for this reason I would like to advice people to activate their roaming when travelling so that they can get real time notifications on withdrawals because it would enable them to notify their bank quickly.

Presented by:

eBotho
for a better e-society

Herding

What is also becoming common is another technique called "herding". As the name suggests,, criminals will temper with an ATM or ATMs in a particular location and then "herd" or direct users to a specific machine they had tampered with. Usually, the criminals would have placed or mounted some skimming devices on that particular machine to copy or clone card information which they then use at a later stage to withdraw funds from people's bank accounts.

Lebanese Loop

Another technique which criminals may use is called "Lebanese loop" whereby criminals insert a thin film in the card slot to trap ATM cards. Users would realise after completing a transaction which required insertion of a card, that the ATM would not eject the card. In truth and reality, the ATM would have ejected the card but it got stuck on the throat of the ATM due to the plastic film. The criminals would then wait for the user to leave the ATM and they would then come and remove the card. In order to access or view your PIN. They would not stand very far and would use another technique called "shoulder surfing" to view you as you enter your PIN. The bank would ordinarily not consider any refund claims for transactions that are chip and pin driven, so act with vigilance at all times. In order to protect your card and PIN from criminals please adhere to the following:

- stand as close as possible to the ATM.
- cover the key pad with your other hand when entering your PIN.
- never accept any assistance from anyone.
- familiarise yourself with the look and feel of the ATM.
- avoid using an ATM which appear to have been tampered with or which has foreign objects attached to it.
- where possible, avoid using offsite ATMs and opt for Branch ATMs
- check your card before leaving an ATM or point of sale after "swipping" your card.
- call the bank immediately when you suspect that your card or pin could have been compromised. Once again, banks may repudiate a claim for a delayed report.

Cyberattacks

Lastly, as more organisations are operating from homes due to the COVID-19 pandemic, their systems have been left vulnerable to cyberattacks as home networks are usually not secure. Criminals are relentlessly making all attempts to gain access to organisations' systems and if not vigilant, you may inadvertently become an enabler. So, be vigilant at all times and be a cyber hero for your organisation by doing the following:

- hang up immediately if you receive an anonymous phone call requesting remote access to your computer.
- avoid clicking on pop-up or virus warning as it could be a scam.
- ensure that you have an up to date antivirus software installed in your computer.
- use VPN when working from home and required to access the organisation's systems..

Supported by:

Universal Access and Service Fund

Botswana Communications Regulatory Authority