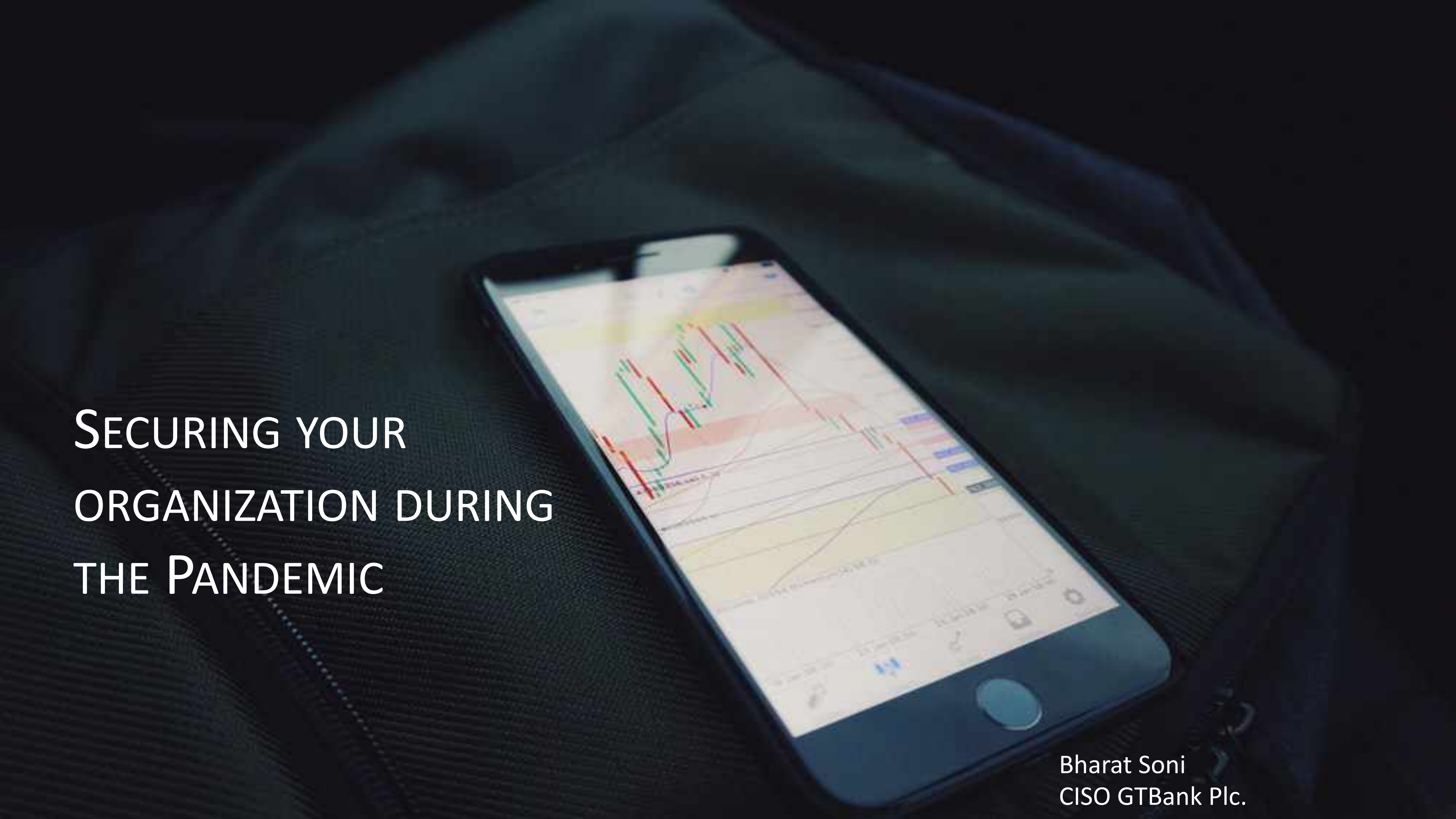
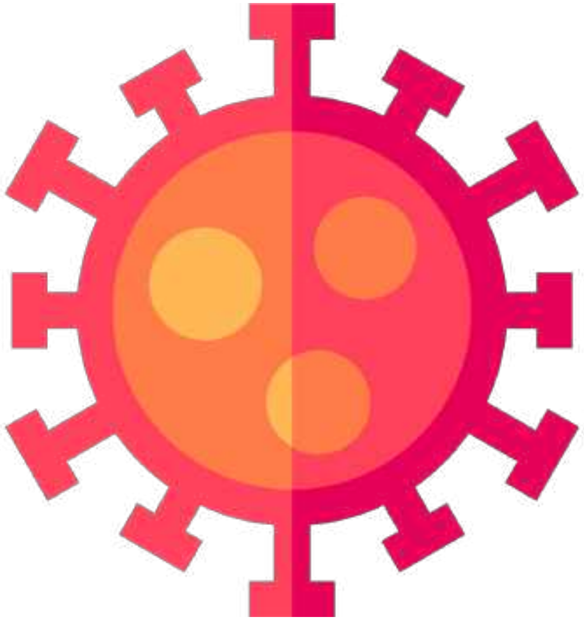


Securing your organization during the Pandemic

Bharat Soni
CISO GTBank Plc.



The ongoing pandemic has transformed nature of work as organizations have expanded their remote access activities and cloud capabilities to an unprecedented level.

Remote Work Activities

Electronic Payments

Cloud storage and applications

Mind boggling statistics at the height of the crisis

800% Increase in reported cybercrimes to the FBI

238% Increase in cyber-attacks against banks is linked to COVID-19

🏛 ⊕ Healthcare and financial sectors were the most targeted.

18million Daily malware and phishing emails blocked by google in April 2020

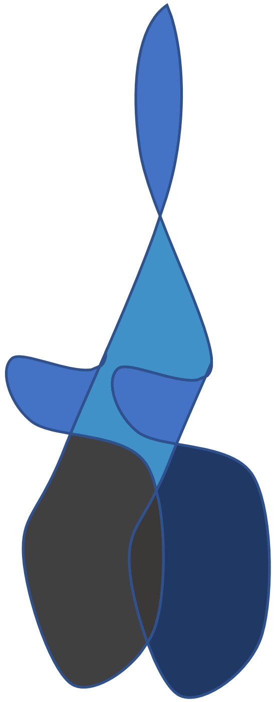
Popular Attack Categories

Online Scams and Phishing

Attacks using phishing increased significantly with many variants arising.

Disruptive Malware (Ransomware and DDoS)

Corporate ransomware attacks were used to cause service disruption.



Data Harvesting Malware

Data exfiltration including sensitive data such as customer details, sensitive designs were targeted data.

Malicious Domains

Some websites and platforms were infected with malware which was then picked up by unsuspecting victims during website visits.

twitter

Attackers compromised the credentials of employees via a social engineering attack, used the initial compromised accounts to compromise more privileged accounts and then used these privileged credentials to access high profile accounts.

130 High profile twitter accounts were accessed including that of Bill Gates, Elon Musk and Joe Biden

$110 Thousand transferred to bitcoin accounts of attackers within minutes of tweet scams being posted.

45 Accounts were tweeted from to promote the bitcoin scam

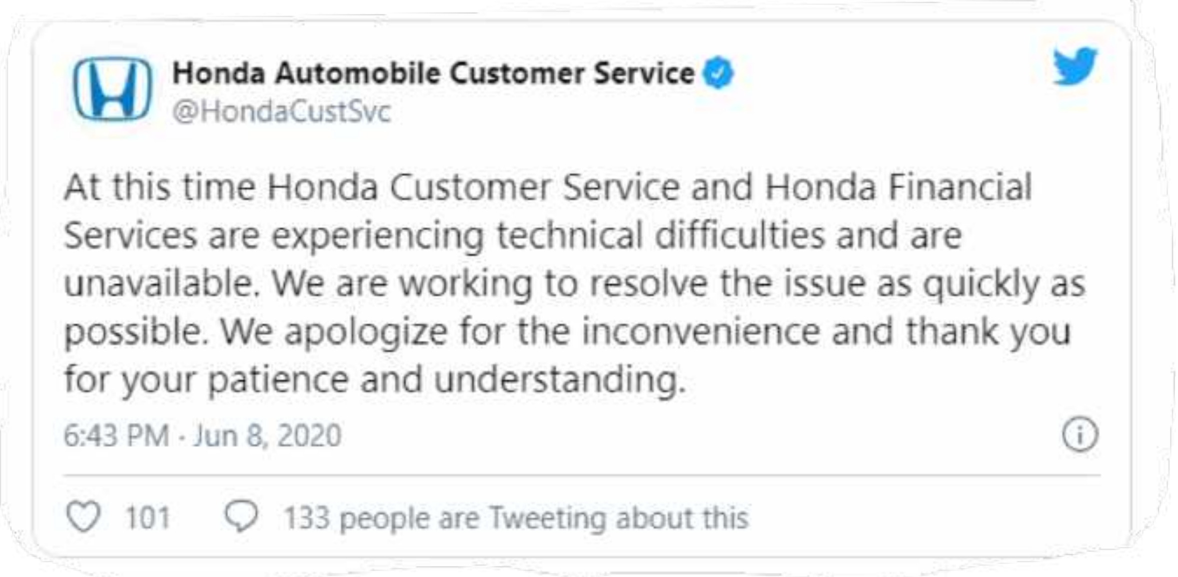
Norfund

In a classic BEC scheme, attackers were able divert loan funds meant for a Cambodian microfinance institution, from a Norwegian state-owned Private Equity Fund

Attackers falsified information exchanged between Norfund and the borrower (including documents and payments details)

$10 Million was eventually transferred to a fraudulent account set up with the same account name as the real account holder.

45+ Days elapsed from when the theft occurred to when it was detected.

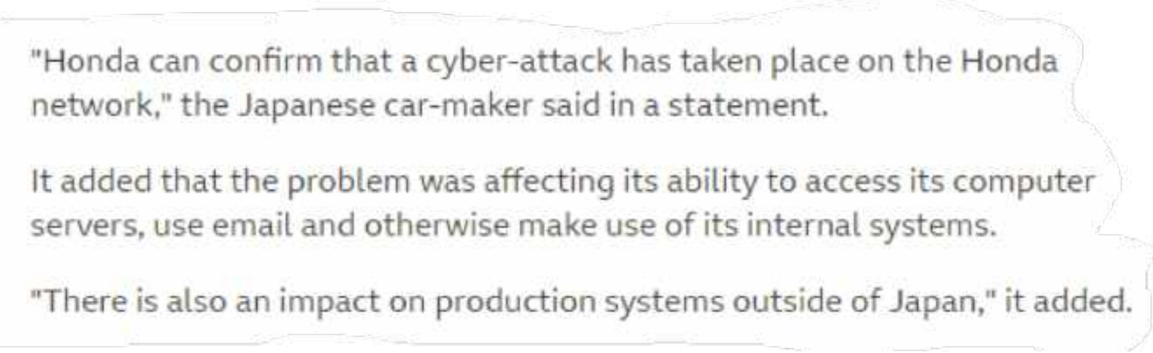


Honda Automobile Customer Service
@HondaCustSvc

At this time Honda Customer Service and Honda Financial Services are experiencing technical difficulties and are unavailable. We are working to resolve the issue as quickly as possible. We apologize for the inconvenience and thank you for your patience and understanding.

6:43 PM · Jun 8, 2020

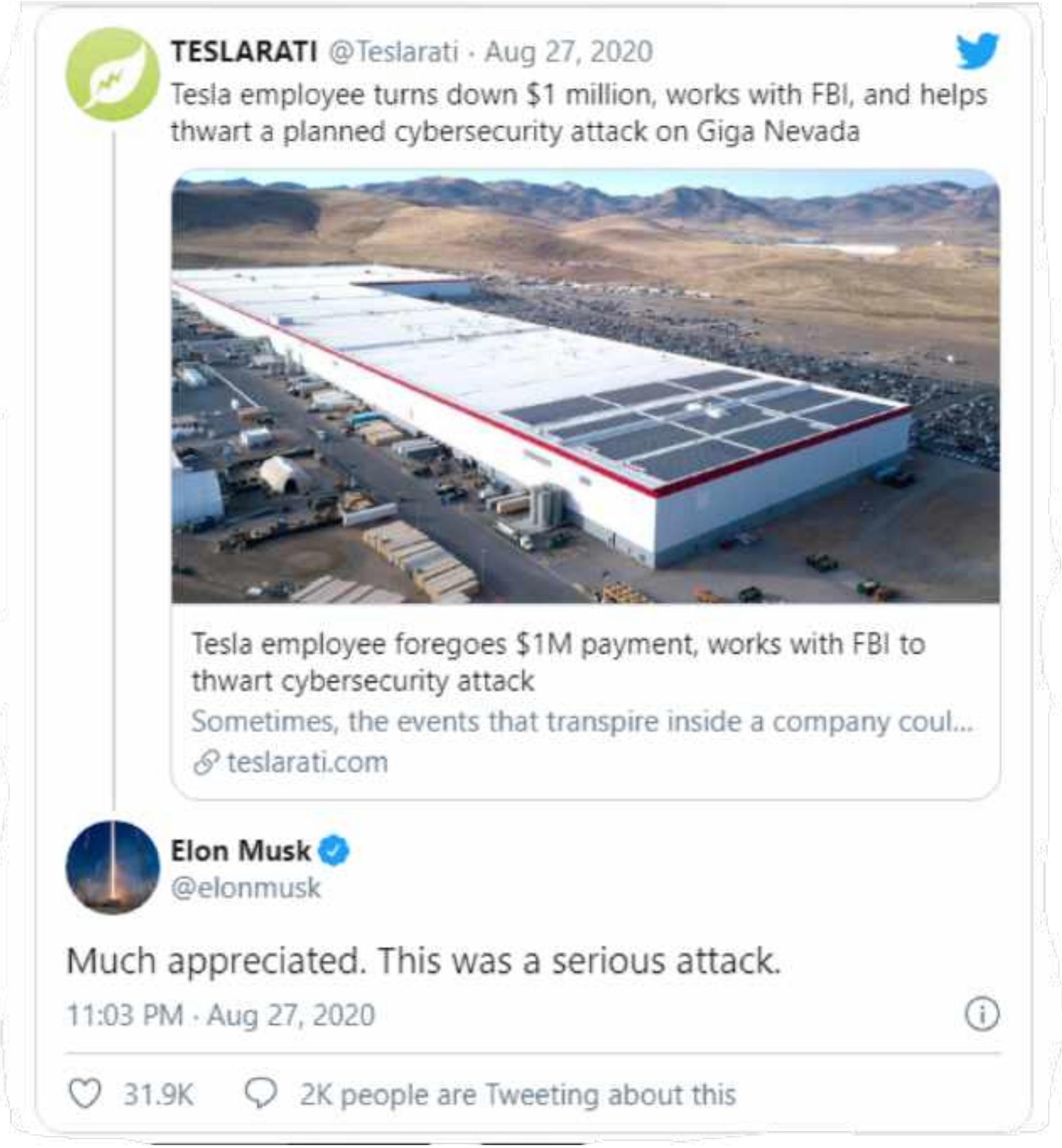
101 133 people are Tweeting about this



"Honda can confirm that a cyber-attack has taken place on the Honda network," the Japanese car-maker said in a statement.

It added that the problem was affecting its ability to access its computer servers, use email and otherwise make use of its internal systems.

"There is also an impact on production systems outside of Japan," it added.



TESLARATI @Teslarati · Aug 27, 2020

Tesla employee turns down $1 million, works with FBI, and helps thwart a planned cybersecurity attack on Giga Nevada

Tesla employee foregoes $1M payment, works with FBI to thwart cybersecurity attack

Sometimes, the events that transpire inside a company coul...

teslarati.com

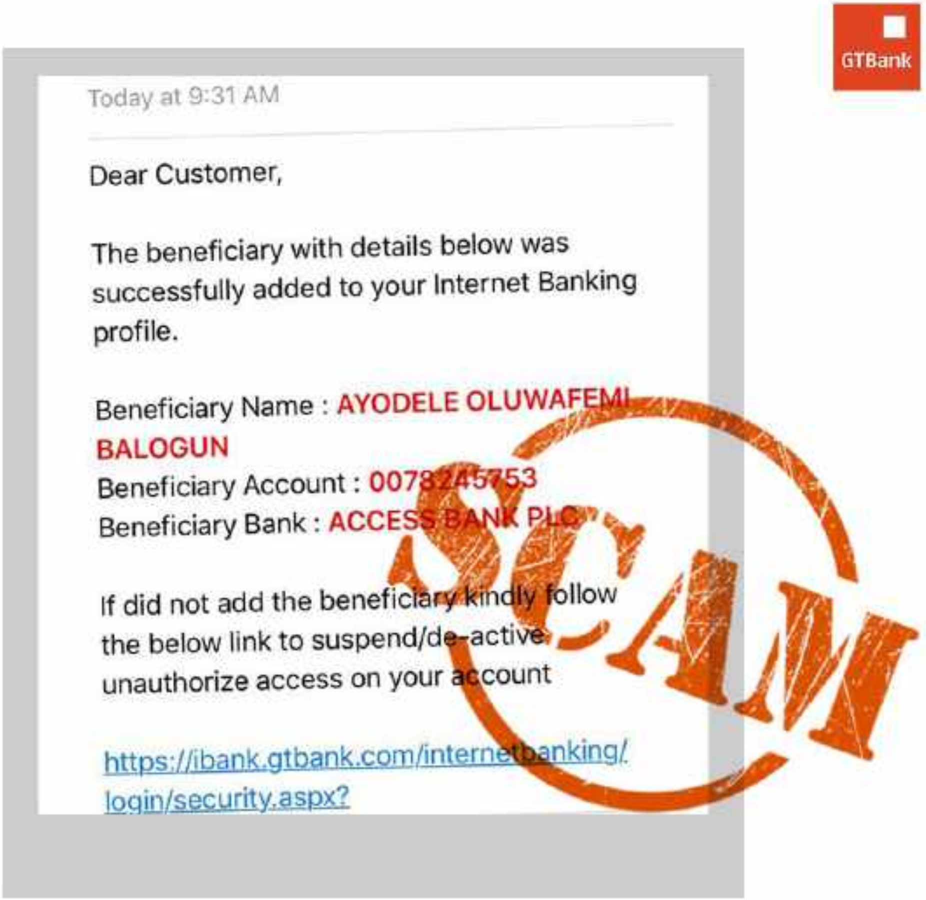
Elon Musk
@elonmusk

Much appreciated. This was a serious attack.

11:03 PM · Aug 27, 2020

31.9K 2K people are Tweeting about this

Phishing Scams on the Rise



Today at 9:31 AM

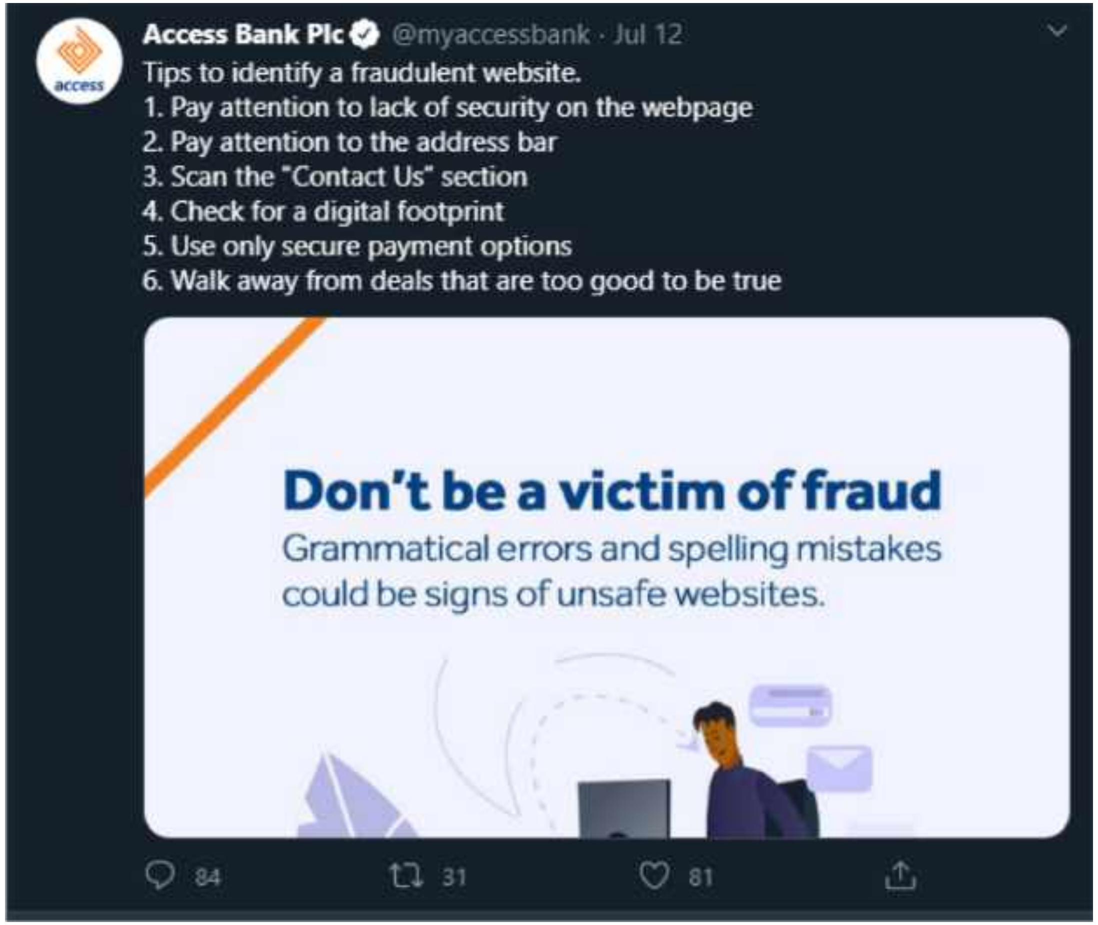
Dear Customer,

The beneficiary with details below was successfully added to your Internet Banking profile.

Beneficiary Name : AYODELE OLUWAFEMI BALOGUN
Beneficiary Account : 0078245753
Beneficiary Bank : ACCESS BANK PLC

If did not add the beneficiary kindly follow the below link to suspend/de-active unauthorize access on your account

https://ibank.gtbank.com/internetbanking/login/security.aspx?



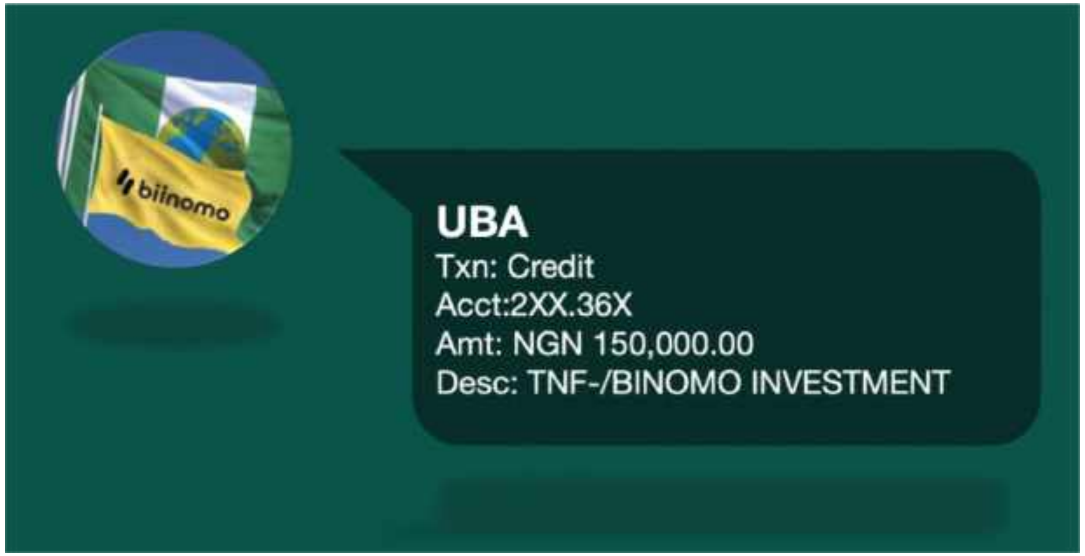
Access Bank Plc @myaccessbank · Jul 12

Tips to identify a fraudulent website.
1. Pay attention to lack of security on the webpage
2. Pay attention to the address bar
3. Scan the "Contact Us" section
4. Check for a digital footprint
5. Use only secure payment options
6. Walk away from deals that are too good to be true

Don't be a victim of fraud

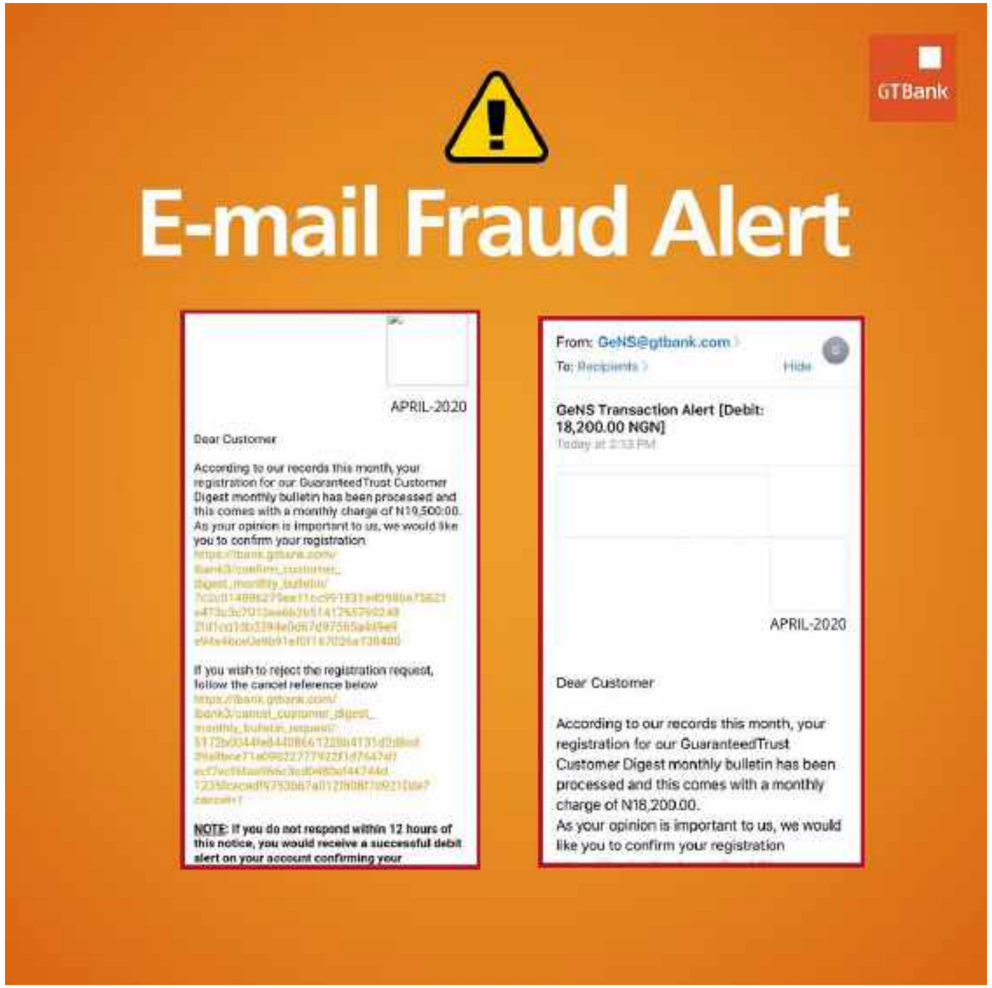
Grammatical errors and spelling mistakes could be signs of unsafe websites.

Phishing Scams on the Rise



UBA
Txn: Credit
Acct:2XX.36X
Amt: NGN 150,000.00
Desc: TNF-/BINOMO INVESTMENT

Binomo Scam in which users' social media accounts are compromised and use to spread false investment payout news to other users to get them to invest in a fraudulent scheme.



APRIL-2020

Dear Customer

According to our records this month, your registration for our GuaranteedTrust Customer Digest monthly bulletin has been processed and this comes with a monthly charge of N19,500:00. As your opinion is important to us, we would like you to confirm your registration
https://ibank.gtbank.com/ibank3/confirm_customer_digest_monthly_bulletin/[illegible]

If you wish to reject the registration request, follow the cancel reference below
https://ibank.gtbank.com/ibank3/cancel_customer_digest_monthly_bulletin_request/[illegible]cancel=1

NOTE: If you do not respond within 12 hours of this notice, you would receive a successful debit alert on your account confirming your

From: GeNS@gtbank.com
To: Recipients
Hide

GeNS Transaction Alert [Debit: 18,200.00 NGN]
Today at 2:13 PM

APRIL-2020

Dear Customer

According to our records this month, your registration for our GuaranteedTrust Customer Digest monthly bulletin has been processed and this comes with a monthly charge of N18,200.00.
As your opinion is important to us, we would like you to confirm your registration

Some organizations are grappling with shrinking budgets as a fallout from the coronavirus crisis making it more difficult for them to allocate cybersecurity spend to protect resources

Necessities in the new world of remote work

Multi-factor authentication

The use of strong authentication for accessing networks has moved from an option to a necessity as it becomes easier for attackers to compromise credentials.

Virtual Private Networks

To facilitate secure transmission of data between employee or third-party devices and organizations, a VPN is required to provide services such as access control, policy enforcement, IP masking and end-to-end encryption.

Protecting the organization

Continuous Monitoring

Monitoring network connections for abnormal behavior, data exfiltration, unusual traffic and other suspicious patterns of compromise have to be reinforced in these times

Security Awareness

Awareness of the new realities of safe cyber practices need to be communicated to employees, partners and customers so that they can remain aware of the evolving cyber threat and how to best protect themselves and your organization.

Protecting the organization

Configuration review

Existing security misconfigurations in systems and infrastructure has become another entry means for attackers into organization’s systems and networks. Thus organizations need to review and monitor such settings regularly to ensure that they offer adequate protection.

Updates and Patching

A lot of organization’s still have systems that are unsupported or missing critical security patches or updates. The shift to work from home has exacerbated it, as a lot of users are connecting with already compromised devices. Organizations need to find ways to address these gaps in order to provide adequate security.

Protecting the organization

Data Loss Prevention

Strategies to address data loss prevention need to be created and adopted by organizations, these include the use of data loss prevention solutions, IRM solutions and the use of CASB solutions to manage multi-cloud environments.

Cyberthreat Intelligence Sharing

The ability to effectively share threat information can help organizations cut down on the dwell time that cybercriminals have on organizations' systems. These involves a collaborative effort from organizations, governments, partners to build a more robust sharing system.

Protecting the organization

Third Party Risk Management

The supply chain of organization has become a hotbed of activities for malicious actors seeking to compromise a target. This means that organizations must look into their connections to vendors, agreements with suppliers to ensure to provide adequate security controls and independent means to assessing the security of partners.

Security Testing & Assessment

Activities to preempt malicious actors such as threat hunting, penetration testing & vulnerability assessments have to be ramped up by organizations seeking to ensure adequate security of their infrastructure and resources.

Thank You