

Avoiding Social Engineering Attacks and Protecting from Cyber Fraud

Content

- **Social Engineering**
- **Social Engineering Methods**
- **Cyber Fraud**



SOCIAL ENGINEERING

Social Engineering

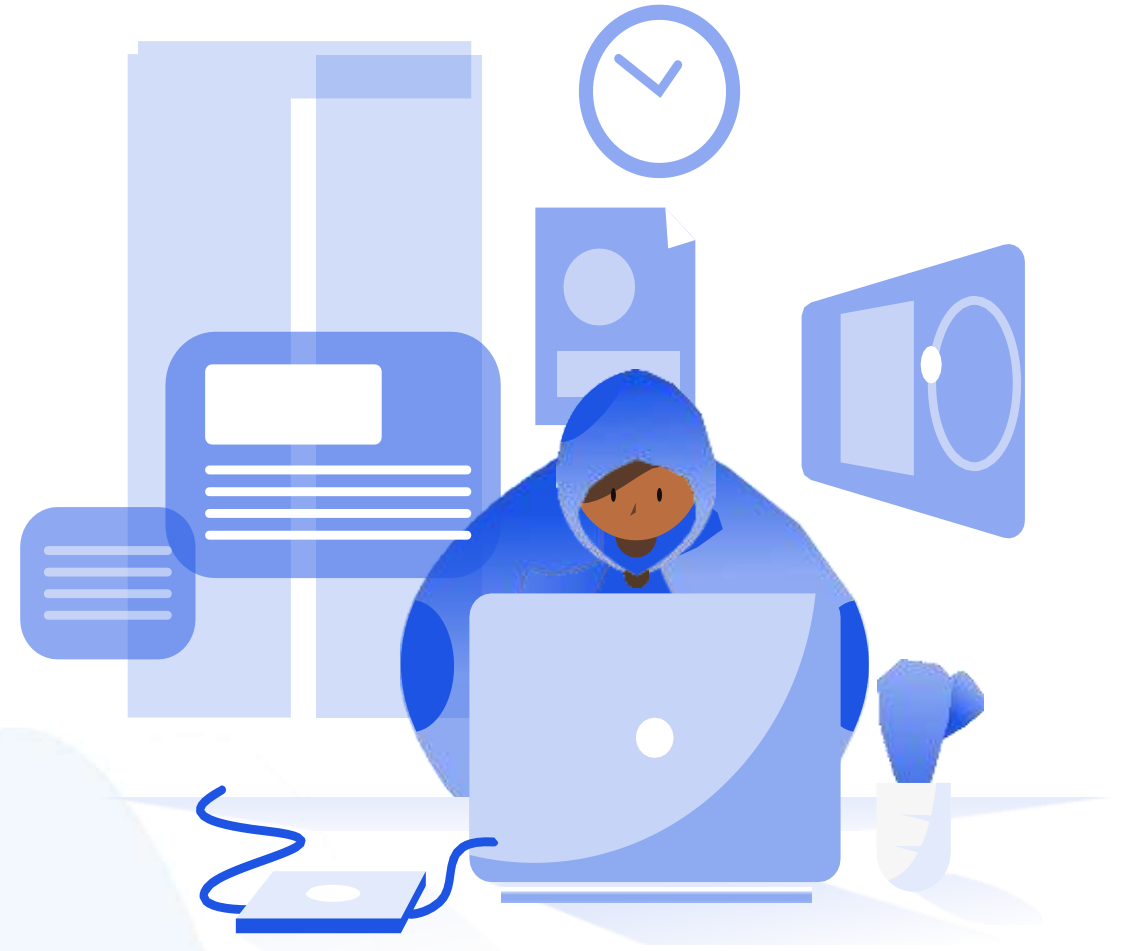
- Psychology of Social Engineering
- Social Engineering Case Study



Psychology of Social Engineering

What is Social Engineering?

The art of psychologically manipulating people into making security mistakes, divulging confidential/sensitive information or taking harmful actions.



Let's take a look at the facts

Nigeria's Consumer Awareness and Financial Enlightenment Initiative had projected a \$6tn loss by 2030 to cybercrime within and outside Nigeria. These crimes are committed mostly through phishing and identity theft.

Social Engineering is the #1 Cyber threat faced in Nigeria

Emotions

**(Desire, Fear, Greed, urgency, Panic,
Excitement, Trust , Curoosity)**

Why hack technology if it's easier to hack a human?

What Do They Want

- Your identity
- Your money
- Sensitive information
- Online accounts



THANK YOU



Social Engineering Case Study

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?



U.S. Citizenship
and Immigration
Services

APPLICATION FOR AMERICAN E-VISA PRESS RELEASE.

President Joe Biden, the 46th U.S. President has signed an Executive Order that interested citizens of the Federal Republic of Kenya, South Africa, Ghana, Tanzania and Ethiopia who measure in some special professions are eligible for American Work E-Visa and Residence Permit. This was communicated to the eligible country commissions in the United States by the U.S Department of Immigration. The Terms of the executive Order allows 25,000 citizens of each eligible country between the age of 25 to 55 whose expertise are among the following: 1. Health Workers, 2. Engineers, 3. Marine Workers, 4. Civil Servants, 5. Business Administrators, 6. Accountants, 7. Lecturers, 8. Special Skills Workers

Interested Qualified Candidates Are Advised to Adhere Strictly to The Following Instructions:

1. All Applicants must send the following documents to the Consular Section via e-mail to info@americaimmigration.us
 - (a) Current (CV) Curriculum Vitae (b) Government Issued I.D or Passport Biodata Page
2. Applicants are advised to monitor their email always for a feedback afterwards. Applicants who do not receive a response after 3 business days should consider their visa applications rejected by the Consular Section and this decision cannot be appealed.
3. Successful Applicants are required to make a deposit of \$250 for English Proficiency Test which must be undertaken in America upon arrival before resumption of any official duty. Children of applicants below the age of 16 are not required to make this payment, however, couples are bound to make payment as principal applicants. Applicants who have not been administered the COVID-19 vaccine must make a deposit of \$150 for COVID-19 screening required before departure to the United States of America and upon arrival.
4. Applicants must go about their applications themselves without involving any third parties such as travel agents, family members living in the United States, or any other delegates.
5. Applicants who wish to be vaccinated upon arrival in the United States do not need to make any payment for vaccines. Vaccination in the United States is free of charge.

Application deadline: 6th of May, 2021.



6th April 2021

Director USCIS



axel springer award

12,362 BTC GIVEAWAY

Elon Musk has personally allocated 12,362 Bitcoins (Worth \$750 Million US Dollars) to be given out as a way to speed up the process of cryptocurrency adoption.

Check the official link or scan the QR code for details.

www.BBC26.com

BBC NEWS TESLA

adidas

Visit advertiser

Skip ad


Congratulations! You have a chance to get free shoes provided by adidas for Women's Day

Congratulations!



You won a pair of SUPERSTAR shoes (please follow the instructions below to claim the prize)



Re: [New Information#60091] Your Account Placed on Hold - March 12, 2021 


 Service Amazing 17:12
to kuku-gogo, bcc: me  



ATM Block: Dear customer your ATM CARD has been blocked due to BVN upgrade of the year quickly call [09055973624](tel:09055973624) to re-activate within 24 hours. 10:21

Forwarded many times

N-Power Nigeria
All N-Power applicants can now check their Examination dates. Input your mobile number on the space provided and then click the check button.
npower-fmhds-gov-ng.web.app



NPOWER SHORTLISTING IS OUT!!!


If you applied for Npower, use this link to check if you are shortlisted for CBT test <https://npower-fmhds-gov-ng.web.app/>

If you are shortlisted, use this link to create an account <https://nasims.gov.ng/login>

Read the entire detail to be able to create an account and login to your dashboard.

10:41 AM

Federal Government Npower Support Fund Program
Get ₦100,000 in The Federal Government Npower Support Fund Program
www.npower-fg-fund.gq

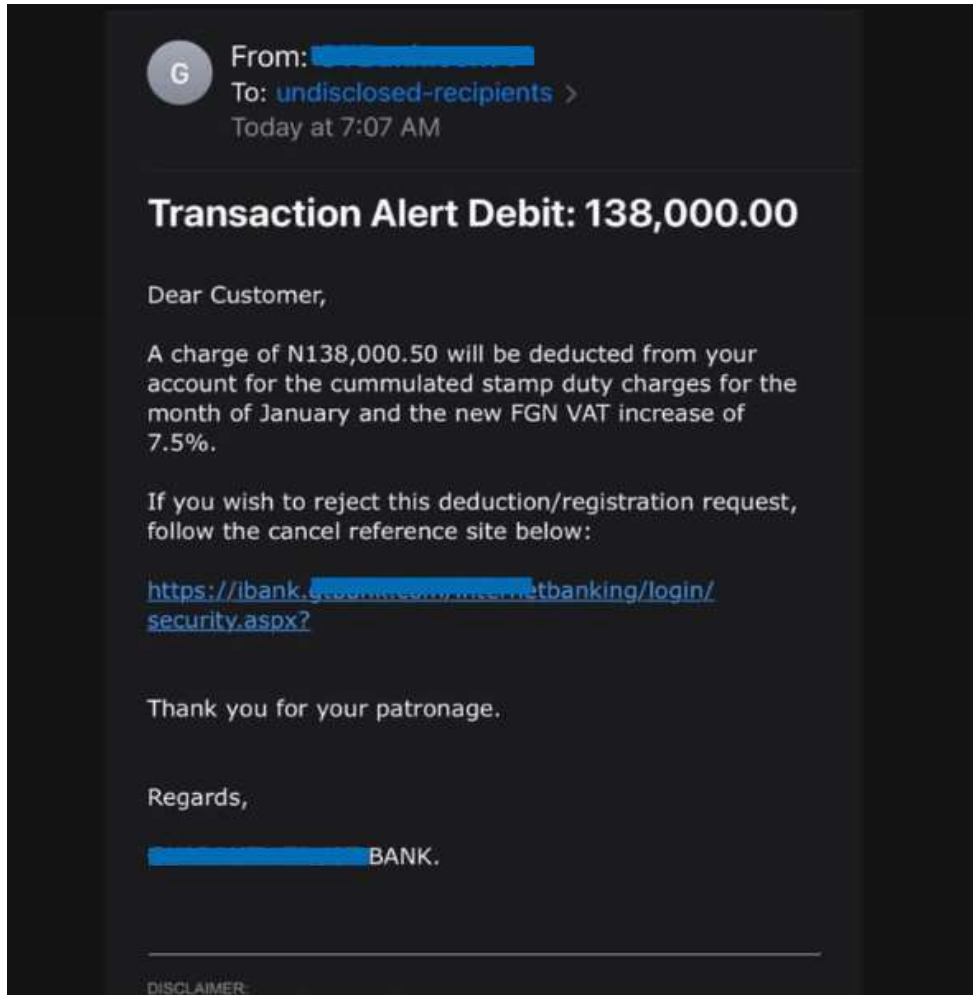


NPOWER GRANT

Dont miss this Federal Governemt ₦100,000 grant. It takes fews seconds to apply. Dont miss this great opportunity.

Apply Here

<https://www.npower-fg-fund.gq/>



From: [redacted] <ghFEDRgrttyuyuyuy667ghghHGFT1556yt@web.de>
To: "Recipients" <ghFEDRgrttyuyuyuy667ghghHGFT1556yt@web.de>
Sent: Mon, Jul 13, 2020 at 10:09
Subject: Add Beneficiary Alert

Dear Customer,

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

Beneficiary Name : **CHIDIEDERE FRANCIS CHUKWURA**
Beneficiary Account : **60238245753**
Beneficiary Bank : **FIDELITY BANK PLC**

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

[https://\[redacted\]etbanking/login/security.aspx?](https://[redacted]etbanking/login/security.aspx?)

Thank you for your patronage.

Regards,

[redacted] K

DISCLAIMER:

Today

Dear Customer, we are running a compulsory security enrollment of all ATM cards issued by banks in Nigeria. CBN as the apex body will block all cards not enrolled within 24hrs of receiving this notification. Visit link: <http://217.71.50.11/~update> to secure your card now.

MTN: ...1 02:53

Your contribution of NGN10,000.00 to your cooperative account has been effected and your voluntary balance is NGN375,000.00.

< F

Text Message
Today 9:29 AM

Congratulations! You are eligible to partake in our pension scheme. As part of your welcome package into the scheme, you will be issued the sum of 100,000 naira. Please visit www.ers.net/registration to claim your gift.

9:00 AM

0704 388 0658

New contact?
Save 0704 388 0658 to your contacts

Add contact Report spam

Yesterday • 3:38 PM

Hi.bukunwi, Gud morning, is me emmanuel eze ur 2021a -copa mate at PL state, am working with (SHELL S. P. D. C.) Oil and Gas Company in Rivers state, Hv u started working if no call me now 4 more details b/cos internal employment is going on now and is very urgent

Hi.bukunmi, Gud morning, is me emmanuel eze ur 2021a -copa mate at PL state, am working with (SHELL S. P. D. C.) Oil and Gas Company in Rivers state, Hv u started working if no call me now 4 more details b/cos internal employment is going on now and is very urgent

Tue 3:39 PM • via Airtel NG

Apply For The Covid-19 Relief Fund Provided By The Federal Government. Hurry Up, It takes few seconds to apply. Dont miss this opportunity.

Apply Here

http://bit.ly/COVID-19-SUPPORT_FUND

18:04

Dont miss this federal government N10,500 weekly grant. It takes few seconds to apply. Dont miss this great opportunity.

Apply Here

<http://bit.ly/Fg-N10500-Weekly>

15:54

FEDERAL GOVERNMENT
SURVIVAL FUND
GET UPTO ₦30,000 CASH PRIZE
IN THE ONGOING SURVIVAL
FUND PROGRAM
survivalfund.online



DON'T MISS ANOTHER FEDERAL GOVERNMENT SURVIVAL FUND GRANT

The Federal Government have reopened the Survival Fund Portal Check if You are Eligible to receive ₦30,000
As Part of SURVIVAL FUND GRANT

Click <https://survivalfund.online/CBN/>

Oya another one don show.
FG go hear am hard hard.
This guys won't just give up so easily

16:31

You have a mysterious gift,
please check 📺

Your gift will expire after 48
hours 📺

sjzjyfs.cn



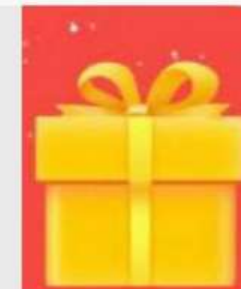
[https://sjzjyfs.cn/tb.php?
app=jrqf&sta=122&lv=2&jrqf1NG=1
99](https://sjzjyfs.cn/tb.php?app=jrqf&sta=122&lv=2&jrqf1NG=199)

10:59

✨ Get Free Giftcards 💕

You have one chance to get free
iPhone12 and other gifts! 📺

bit.ly



[https://bit.ly/WinAmazonGiftcards?
c=www.amazon.com](https://bit.ly/WinAmazonGiftcards?c=www.amazon.com)

🕒 Amazon 30th anniversary celebration 🙌

Free gifts for everyone!

amasozm.xyz

[http://amasozm.xyz/amazon/
tb.php?v=ss1616609](http://amasozm.xyz/amazon/tb.php?v=ss1616609)

19:11

💰 80th anniversary celebration

💕 Everyone can get free gifts

jifkpyq.asia



[https://jifkpyq.asia/nestle-bx/?
t=1617744443604](https://jifkpyq.asia/nestle-bx/?t=1617744443604)

15:08



THANK YOU



SOCIAL ENGINEERING METHODS

Social Engineering Methods

- **Phishing & Spotting Phishing**
- **Phishing Types**
- **Other Social Engineering Methods**
- **Impact of Social Engineering**



Phishing & Spotting Phishing Emails

Social Engineering Tricks

- **Gaining trust by providing some information- familiar nature (rapport building)**
- **Helpfulness (presents a problem then becomes the saviour)**
- **Steer emotions**
- **Offering rewards**
- **Urgency**
- **Stirs fear**
- **Unrealistic threat or consequence**
- **Asks you to break protocol**

Phishing

Phishing is deception through email which aims to get victims to reveal sensitive information, click on harmful links or open attachments that contain harmful software by disguising as a trustworthy entity in an email.

How to Spot Phishing Emails

- **Generic greetings**
- **Spelling & grammatical errors**
- **They induce extreme emotions**
- **Dangerous file attachments**
- **Contains offers that are too good to be true**
- **Misspelt domain name**
- **Malicious links**
- **Inconsistencies in email address, links and domain names**
- **Requests for sensitive information.**

Can you detect a phishing mail?

Take This Quiz

<https://phishingquiz.withgoogle.com/>



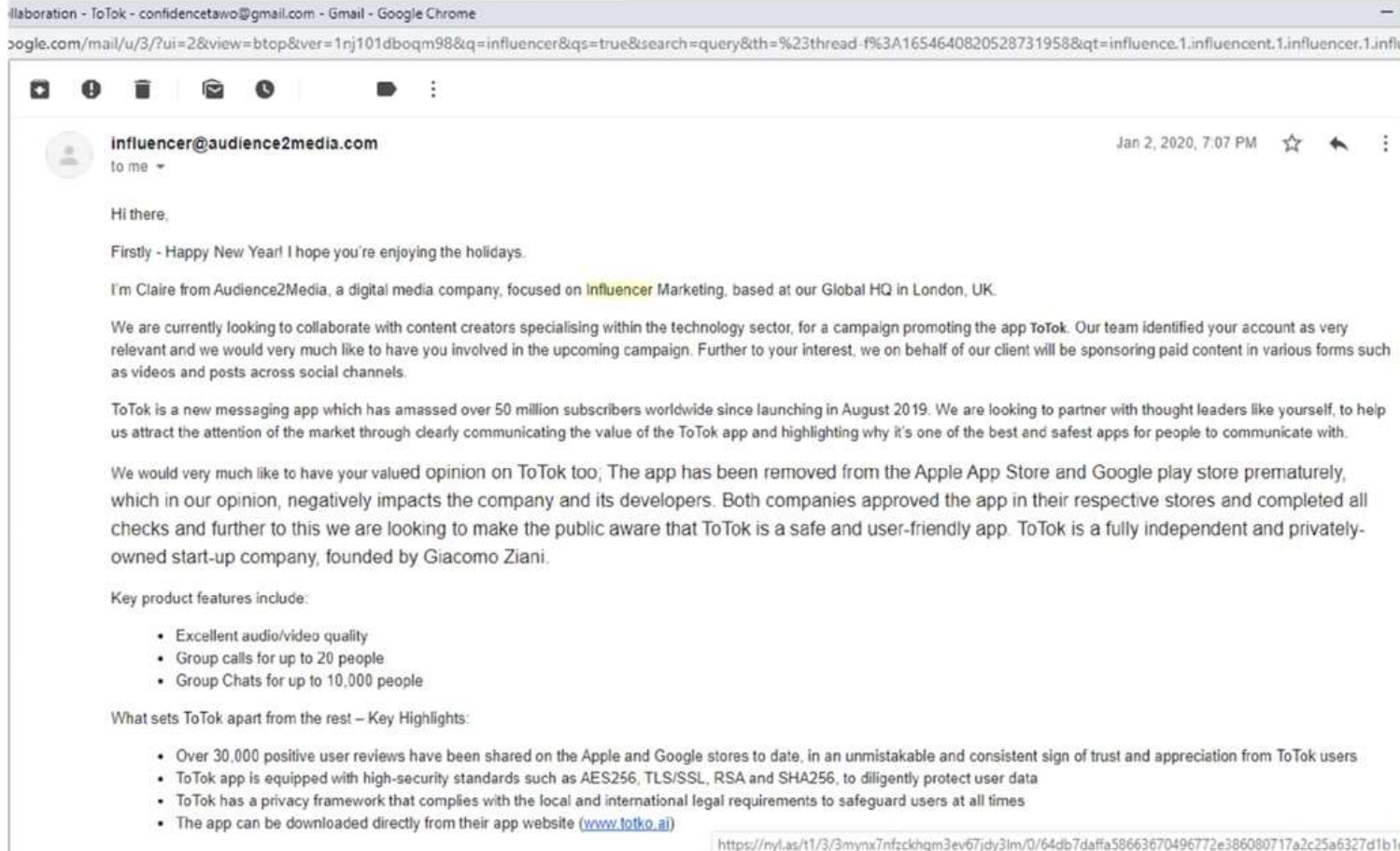


THANK YOU



Phishing Types

Spear Phishing



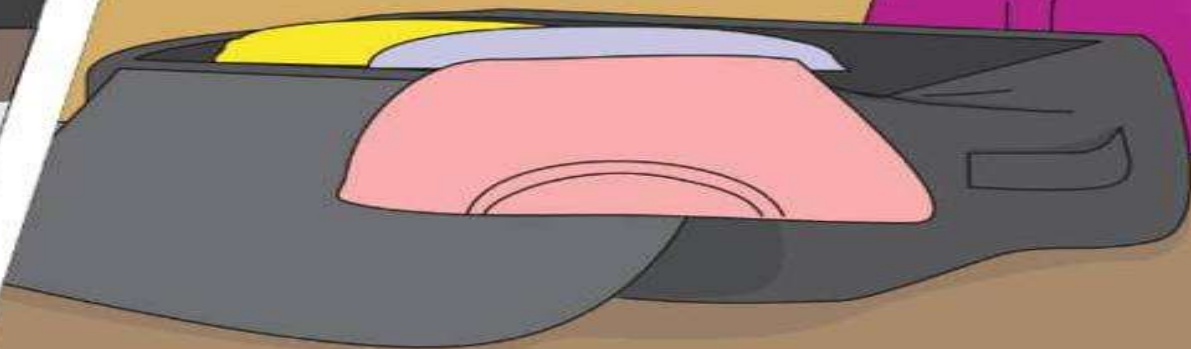
A more targeted version of the phishing scam whereby an attacker chooses specific individuals within an organization. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous.

Vishing

Often referred to as voice phishing, vishing is a deception method cybercriminals use savvy deceptive tactics to convince victims to act, giving up private information and access to bank accounts.



YOUR
BANK, WILL
NEVER ASK FOR
YOUR PIN, CVV,
COMPLETE CARD
NUMBER, VERIFICATION
CODE OR ONE TIME
PASSWORD



Vishing

Smishing is a social engineering attack carried out over mobile text messaging, also known as SMS phishing. Victims are deceived into giving sensitive information to a disguised attacker. It occurs on many mobile text messaging platforms, including non-SMS channels like data-based mobile messaging apps like WhatsApp.



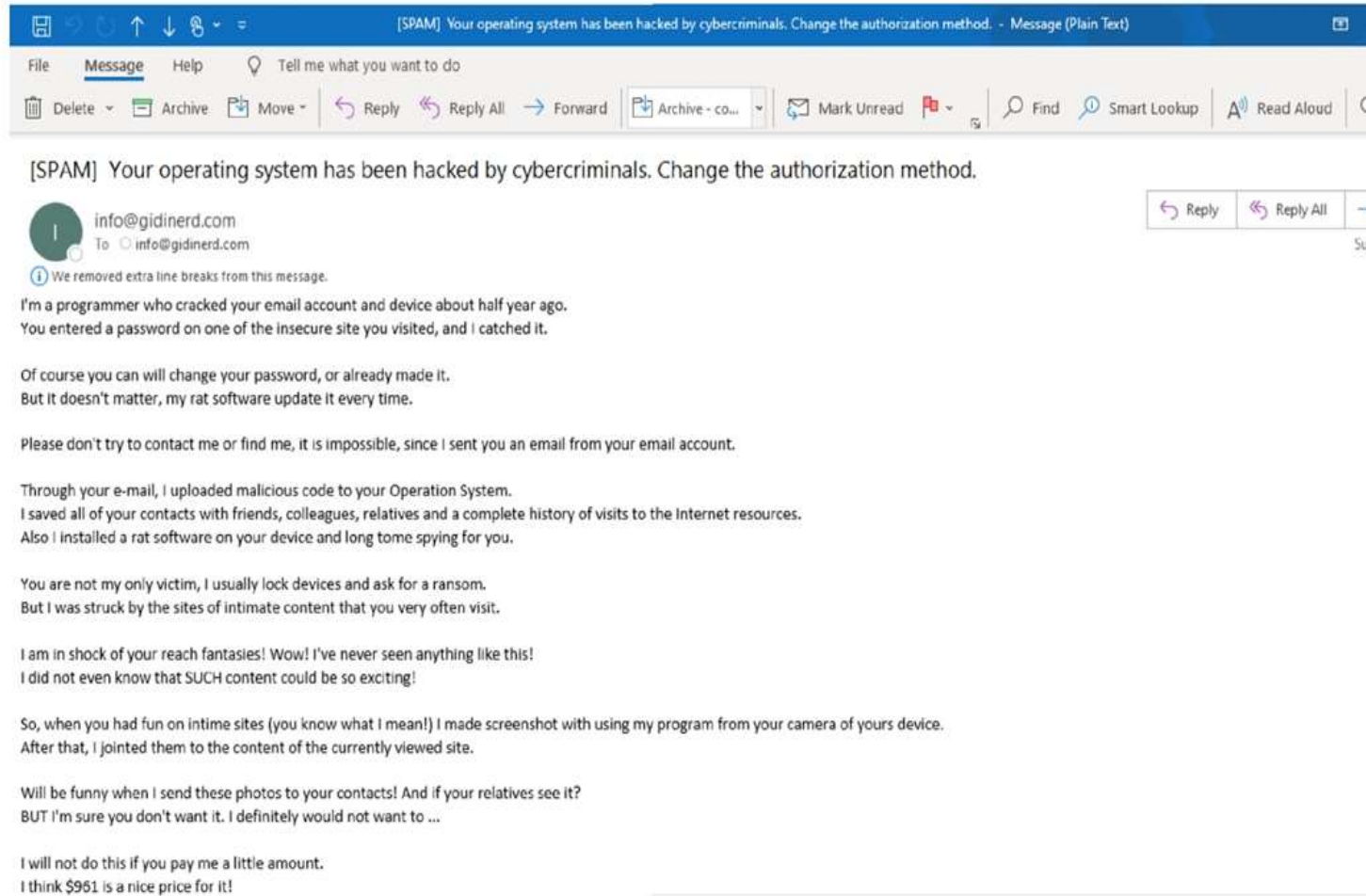


THANK YOU



Other Social Engineering Methods

Pretexting



Someone pretends to need sensitive information from you for an alleged critical task.


Spooftng


[SPAM] Your Shipment is available for pickup - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Move Reply Reply All Forward Archive - co... Mark Unread Find Smart Lookup Read Aloud

[SPAM] Your Shipment is available for pickup

 DHL Notification <No-response948857773@dhl.com>
To confidence@gidinerd.com



Dear Customer,

Ref: 3559920 (Delivery Attempt Failures)- Reason: Incomplete Delivery Address.

Your parcel dispatched via DHL on 02/05/2020 has arrived and is now available for delivery but we are unable to locate your delivery address as contained in our manifest.

Content of Parcel: Shipping Documents/Original BL, Invoice & Packing List

Sender: Maersk Shipping
Scheduled Delivery Date: 2020-04-05 14:30:00
Service: P
Pieces: 1
Cust. Ref: 724420
Description: Documents

Click [Here](#) to verify and confirm your delivery address.

Sitemap: Accessibility: Legal Notice: Terms of Use: Privacy Notice: Using DHL Websites: Dispute Resolution: 2020 © DHL International G
rights reserved.

Pretending
to be
someone
you are not

Baiting

Baiting involves luring an unsuspecting victim with a highly attractive offer playing on fear, greed and temptation to make them part with their personal sensitive data like log-in details. Through fraudulent, fake methods, both attempt to capture confidential, personal details such as a password or banking information such as a PIN so they can access your business networks and systems to instal malware which executes ransomware.



Topic Activity

Spot the difference

www.netflix.com



www.netfliix.com



Topic Activity

Spot the difference

www.npower-fp-fund.gq 🔍

www.npower.org 🔍



THANK YOU



Impact of Social Engineering

Business Email Compromise

This is a social engineering method that targets companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers, resulting in massive losses.

Business Email Compromise

An impersonation attack typically involves an email that seems to come from a trusted source. like the CEO, CFO or another high-level executive, a trusted colleague, a third-party vendor or other well-known Internet brands requesting you to perform certain financial transactions.

Preventing Business Email Compromise

- **Process information and determine truth**
- **Be wary of tempting offers**
- **Trust but verify: Multi-channel request verification**
- **Manually type out web addresses. Make a habit not to click links in emails.**
- **Review sender's email address**
- **Scan attachments for malware**
- **Keep your antivirus/antimalware software updated**
- **Use multi-factor authentication**
- **Build a culture of not circumventing due process**
- **Ensure vendor security**

Social Engineering Trends

- Use of shortened URLs
- Combination of Smishing and Vishing
- Baiting with relevance e.g. using seasonal celebration, global events, trending announcements, etc.
- Impersonation
- Targeted emails (Spear phishing)
- Lookalike domains and websites
- Adware/banking malware e.g. trojans
- Opportunity scams
- Investment Scams
- Sponsored social media ads

How To Stay Safe

- **Stop and think**
- **Verify authenticity**
- **Assess – senders name**
- **Zero trust mindset**
- **Scan links in emails or attachment**
- **Turn on 2FA and have a strong password**
- **Download apps only from your app store**
- **Have an antivirus installed**

Activity Break

Do this if that email contains a link
or attachment

<https://virustotal.com/>





THANK YOU



CYBER FRAUD

Cyber Fraud

Cyber Fraud and Types

Types of Cyber Fraud Part 2

Types of Cyber Fraud Part 3

Cyber Fraud Preventive Measures



Cyber Fraud and Types

What is Cyber fraud?

Cyber fraud is the use of internet services and a computing device by cybercriminals to defraud another individual, gain access to a victims' personal identity, corrupt their personal and financial information stored online or otherwise take advantage of them.

Cyber fraud is the most common type of fraud and the extensive and popular use of internet banking and mobile banking means there are more opportunities than ever for criminals to commit cyber fraud.

Types of Cyber Fraud

Frequent instances of cyber fraud include;

- **Business Fraud**
- **Credit Card Fraud**
- **Internet Auction Fraud**
- **Investment Schemes**
- **Nigerian Letter Fraud**
- **Cryptojacking**
- **Identity Theft**
- **Software Piracy**
- **Cyberespionage**
- **Cyberextortion**
- **Exit Scam**
- **Non-delivery Of Merchandise**

Types of Cyber Fraud

Business Fraud

Business fraud consists of dishonest and illegal activities perpetrated by individuals or companies in order to provide an advantageous financial outcome to those persons or establishments. Also known as corporate fraud, these schemes often appear under the guise of legitimate business practices. An array of crimes fall under business fraud, including the following:

- **Charity fraud:** Using deception to get money from individuals believing they are making donations to legitimate charity organizations, especially charities representing victims of natural disasters shortly after the incident occurs.
- **Internet auction fraud:** A fraudulent transaction or exchange that occurs in the context of an online auction site.

Types of Cyber Fraud

- **Non-delivery of merchandise:** Fraud occurring when a payment is sent but the goods and services ordered are never received.
- **Non-payment of funds:** Fraud occurring when goods and services are shipped or rendered but payment for them is never received.
- **Overpayment scheme:** An individual is sent a payment significantly higher than an owed amount and is instructed to deposit the money in their bank account and wire transfer the excess funds back to the bank of the individual or company that sent it. The sender's bank is usually located overseas, in Eastern Europe for example, and the initial payment is found to be fraudulent, often after the wire transfer has occurred.
- **Re-shipping scheme:** An individual is recruited to receive merchandise at their place of residence and subsequently repackage the items for shipment, usually abroad. Unbeknownst to them, the merchandise was purchased with fraudulent credit cards, often opened in their name.



THANK YOU

Types of Cyber Fraud

Part 2

Types of Cyber Fraud

Credit Card Fraud

Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property. Credit and debit card numbers can be stolen from unsecured websites or can be obtained in an identity theft scheme.



Types of Cyber Fraud

Internet Auction Fraud

Internet auction fraud involves schemes attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Non-delivery of Merchandise

Non-delivery of merchandise is a scheme most often linked to Internet auction fraud, in which a seller on an Internet auction website accepts payment for an item yet intentionally fails to ship it. Sellers like these sometimes will relist the item and attempt to sell it again through a different username. Non-delivery of merchandise can also be considered a form of business fraud in a number of

Types of Cyber Fraud

Investment Fraud

Investment fraud involves the illegal sale or purported sale of financial instruments. The typical investment fraud schemes are characterized by offers of low- or no-risk investments, guaranteed returns, overly-consistent returns, complex strategies, or unregistered securities. Examples of investment fraud include advance fee fraud, Ponzi schemes, pyramid schemes, and market manipulation fraud.

These schemes often seek to victimize affinity groups—such as groups with a common religion or ethnicity—to utilize the common interests to build trust to effectively operate the investment fraud against them. The perpetrators range from professional investment advisers to persons trusted and interacted with daily, such as a neighbor or sports coach.

Types of Cyber Fraud

Nigerian Letter Frauds

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed, or e-mailed, from Nigeria offers the recipient the “opportunity” to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number given in the letter or return e-mail address provided in the message. The scheme relies on convincing a willing victim, who has demonstrated a “propensity for larceny” by responding to the invitation, to send money to the author of the letter in Nigeria in several instalments of increasing amounts for a variety of reasons.



THANK YOU

Types of Cyber Fraud

Part 3

Types of Cyber Fraud

Cryptojacking

Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Like many forms of cybercrime, the motive is profit, but unlike other threats, it is designed to stay completely hidden from the victim.

Identity Theft

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Types of Cyber Fraud

Cyber Extortion

Cyber extortion is the act of cyber-criminals demanding payment through the use of or threat of some form of malicious activity against a victim, such as data compromise or denial of service attack. Cyber extortion permeates actions such as ransomware, email ransom campaigns, and distributed denial of service (DDoS) attacks.

Types of Cyber Fraud

I captured a video from your screen and the camera of the device. I edited a video wherein one part of the screen there is a video of you masturbating and in the other a pornographic video that you opened at that time. I can see all the contacts from your phone and all of your social networks.

At one moment, I can send this video to all the contacts on your phone, email, and social networks. Moreover, I can also send your email and messenger data to everybody.

I can destroy your reputation forever.

If you want to avoid this, then:
Send 1500 USD (USA dollars) to my bitcoin wallet

Types of Cyber Fraud

Software Piracy

Software piracy is the illegal copying, installation, use, distribution, or sale of software in any way other than that is expressed in the license agreement. The software industry is facing huge financial losses due to the piracy of software. Piracy of software is performed by end-users as well as by the dealers.



Types of Cyber Fraud

Exit Scam

An exit scam is a confidence trick where an established business stops shipping orders while receiving payment for new orders. If the entity had a good reputation, it could take some time before it is widely recognized that orders are not shipping, and the entity can then make off with the money paid for unshipped orders.

Cyberespionage

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Types of Cyber Fraud

Exit Scam

An exit scam is a confidence trick where an established business stops shipping orders while receiving payment for new orders. If the entity had a good reputation, it could take some time before it is widely recognized that orders are not shipping, and the entity can then make off with the money paid for unshipped orders.

Cyberespionage

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.



THANK YOU



Cyber Fraud Preventive Measures

How to Prevent Cyber Fraud

- **Continually update your computer and mobile devices.**
- **Use good password habits**
- **Restrict access to your computer and devices by using passwords and multiple computer profiles**
- **Talk to your children and family about internet security.**
- **Know what to do if you become a victim.**
- **Activate your firewall – Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.**
- **Use anti-virus/malware software – Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.**

How to Prevent Cyber Fraud

- Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
- Check your security settings and be careful what information you post online.
- Be aware that your mobile device is vulnerable to viruses and hackers.
- Be aware that your mobile device is vulnerable to viruses and hackers.
- Download applications from trusted sources. Install the latest operating system updates. Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates.
- Turn on automatic updates to prevent potential attacks on older software.
- Make regular back-ups of all your important data, and store it in another location.

How to Prevent Cyber Fraud

- **Secure your wireless network. Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured**
- **Review and modify default settings.**
- **Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.**
- **Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet.**

How to Prevent Cyber Fraud

- **Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).**
- **Always think before you click on a link or file of unknown origin.**
- **Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source.**
- **Never reply to emails that ask you to verify your information or confirm your user ID or password.**



THANK YOU