PHISHING AND FINANCIAL FRAUDS

BY- KHOOSHI SETH
LEGAL INTERN
SETH ASSOCIATES

PHISHING

Phishing is described as a fraudulent activity that is committed to steal confidential user information such as credit card numbers, login credentials, and passwords. It is usually committed by using email or other forms of electronic communication by pretending to be from a reliable business entity.


Deceptive Phishing
Spear Phishing
Whaling
Pharming
Smishing
Vishing
Clone Phishing
Snow-shoeing
Phishing Attacks

Types of Phishing:

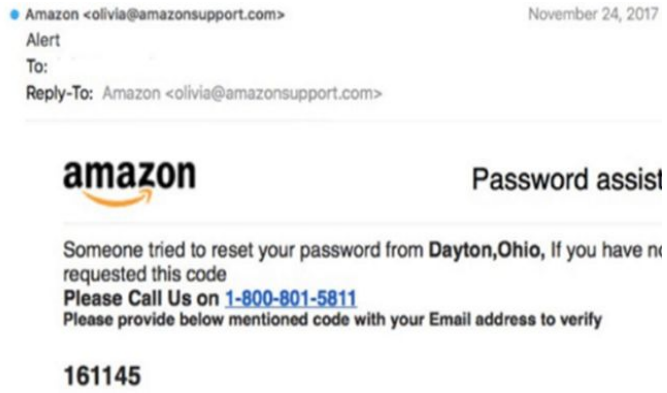
1. Email phishing

Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organisation and sends thousands of generic requests.

The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.

In other cases, the fraudsters create a unique domain that includes the legitimate organisation's name in the URL. The example below is sent from 'olivia@amazonsupport.com'.The recipient might see the word 'Amazon' in the sender's address and assume that it was a genuine email.

There are many ways to spot a phishing email, but as a general rule, you should always check the email address of a message that asks you to click a link or download an attachment.

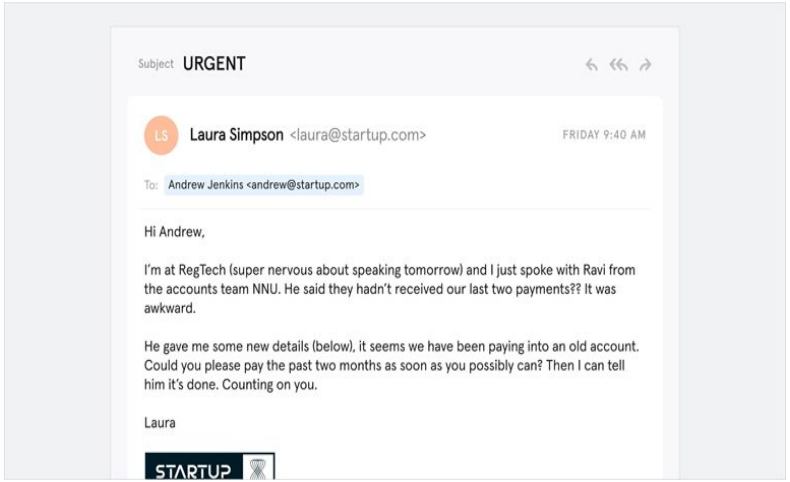


2. Spear phishing

There are two other, more sophisticated, types of phishing involving email.

The first, spear phishing, describes malicious emails sent to a specific person. Criminals who do this will already have some or all of the following information about the victim:

- Their name.
- Place of employment.
- Job title.
- Email address; and
- Specific information about their job role.



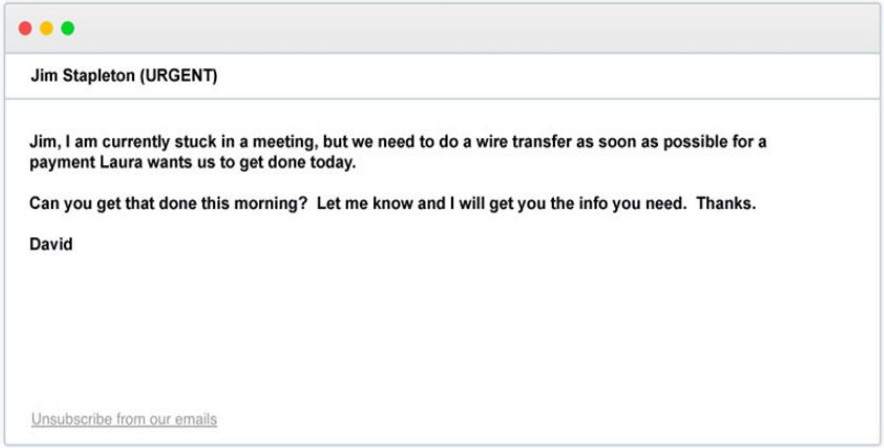
The fraudster addresses the individual by name and (most often) knows that their job role involves making bank transfers on behalf of the company.

The informality of the email also suggests that the sender is a native English speaker and creates the sense that this is a real message rather than a template.

3. Whaling

Whaling attacks are even more targeted, taking aim at senior executives. Although the end goal of whaling is the same as any other kind of phishing attack, the technique tends to be a lot subtler.

Tricks such as fake links and malicious URLs aren't helpful in this instance, as criminals are attempting to imitate senior staff.



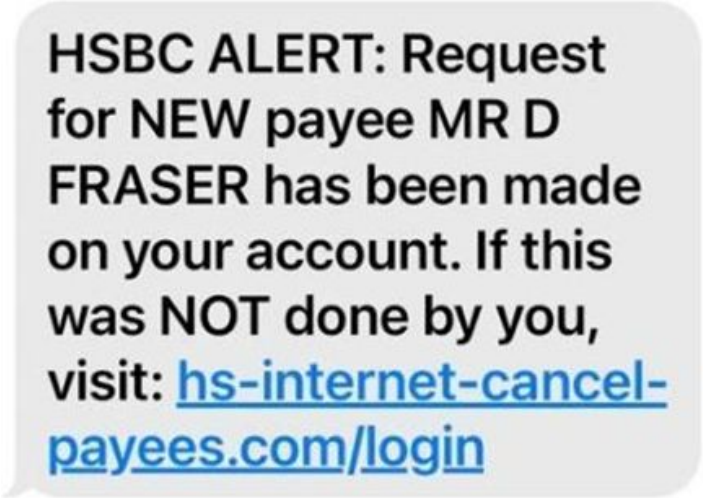
4. Smishing and vishing

With both smishing and vishing, telephones replace emails as the method of communication.

Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.

One of the most common smishing pretexts are messages supposedly from your bank alerting you to suspicious activity.

In this example, the message suggests that you have been the victim of fraud and tells you to follow a link to prevent further damage. However, the link directs the recipient to a website controlled by the fraudster and designed to capture your banking details.



How to prevent phishing scams:

1. Protect your computer by using security software. Set the software update to 'automatic' so it will deal with any new security threats.

2. Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:

- **something you know — like a passcode, a PIN, or the answer to a security question.**
- **something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key**
- **something you are — like a scan of your fingerprint, your retina, or your face**

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Backup your computers data to an external hard drive or in the cloud. Back up the data on your phone, too.

Tips to Prevent Phishing Attacks:

Know what phishing scams look like.

Get free anti-phishing add-ons

Don’t give your information to an unsecured site

Rotate passwords regularly

Install firewalls

Don’t be tempted by those pop-ups

Don’t give out important information unless you must

Have a Data Security Platform to spot signs of an attack

Don’t click on random links

FINANCIAL FRAUD

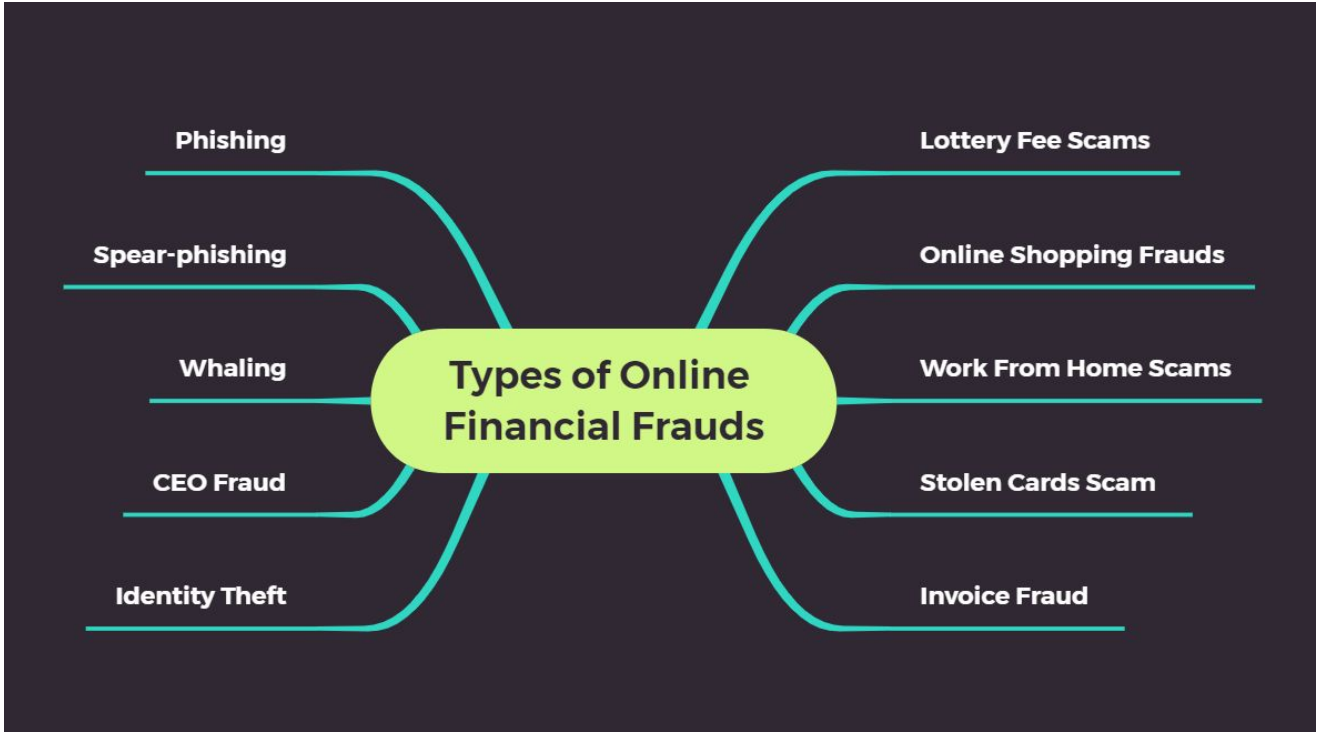
Financial fraud occurs when someone takes money or other assets from you through deception or criminal activity. These scams can occur in relation to credit cards, debit cards, ATM, online payment and business transactions.

Today, India ranks second only to China, with more than 690 million active internet users which constitute almost 41% of our country's total population. On the back of this massive digital penetration, many services have flourished in both rural and urban India, particularly online banking.

Digital payments and online banking are sectors that have witnessed a tremendous boost with consumers preferring to transact online given the ease that it offers. We have witnessed a massive surge in banking and cyber frauds where both consumers and banks have been affected. Hence, it is important to create awareness about fraudsters and continue to take steps to curb their actions.

Source: www.economictimes.in

Central Banks across the world have reported that these frauds have become more sophisticated and have been increasing in numbers. The amount of money involved in these frauds has also increased. Indian banks are continuously and effectively taking measures to raise awareness among consumers and have updated their technology to deal with cyber attacks.



A primary effect of cybercrime is financial. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information.

IMPORTANT INFORMATION:

You should report the financial fraud within 24 hours of occurrence.You need to report it to Police on www.cybercrime.gov.in.

1930 is the financial fraud helpline number

This reporting platform has been made operational by the Indian Cyber Crime Coordination Centre (14C) under the Ministry of Home Affairs, with active support and cooperation from the Reserve Bank of India (RBI), along with all major banks, payment banks, wallets, payment gateways and online merchants.

Citizen Financial Cyber Frauds Reporting and Management System

As cyber crime continues to increase, banks and financial institutions have adopted a proactive approach to cybersecurity. Financial fraud and identity theft can be effectively beaten given that banks are already investing heavily in a robust security infrastructure along with educating their customers. The Reserve Bank of India is very proactive in conducting drives around financial awareness.

Steps for reporting of financial cyber frauds:

i) Any victim of financial cyber fraud can dial helpline number 1930 or report the incident on National Cybercrime Reporting Portal (www.cybercrime.gov.in)

ii) A Bank or financial intermediary or payment wallet can also report financial cyber fraud through above-mentioned modes.

iii) On receipt of complaint, the designated Police Officer will quickly examine the matter and investigate. You can also report the fraud to concerned Bank/financial intermediary or payment wallet, etc., for blocking the money involved in the financial cyber fraud and blocking any debit/credit cards.

iv) Thereafter, due action as per law will be taken in each case by Police/Bank/Payment wallet/Financial Intermediary.

vii) Use of this facility will help a victim of financial cyber fraud in retrieving the money and help Police in identifying the cyber criminal(s) and take legal action as per law

Source: www.cybercrime.gov.in

Cyber empowerment for one and all!

Q& A Round!

Khooshi Seth
Legal Intern
Seth Associates