Social Engineering

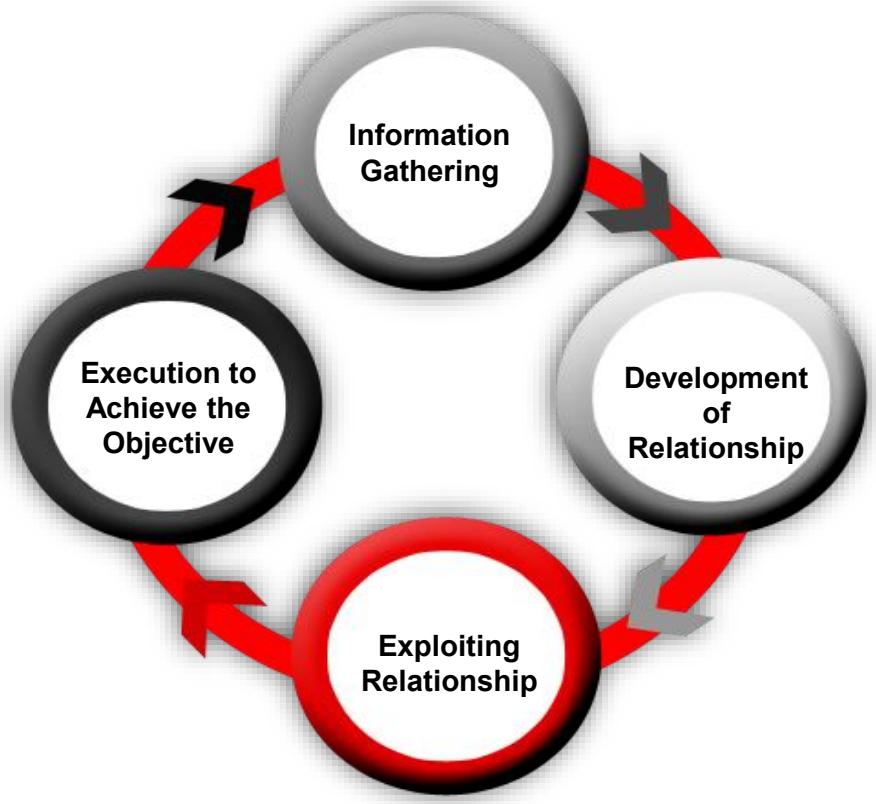
Cybersecurity Awareness

About

Social Engineering

What is Social Engineering ?

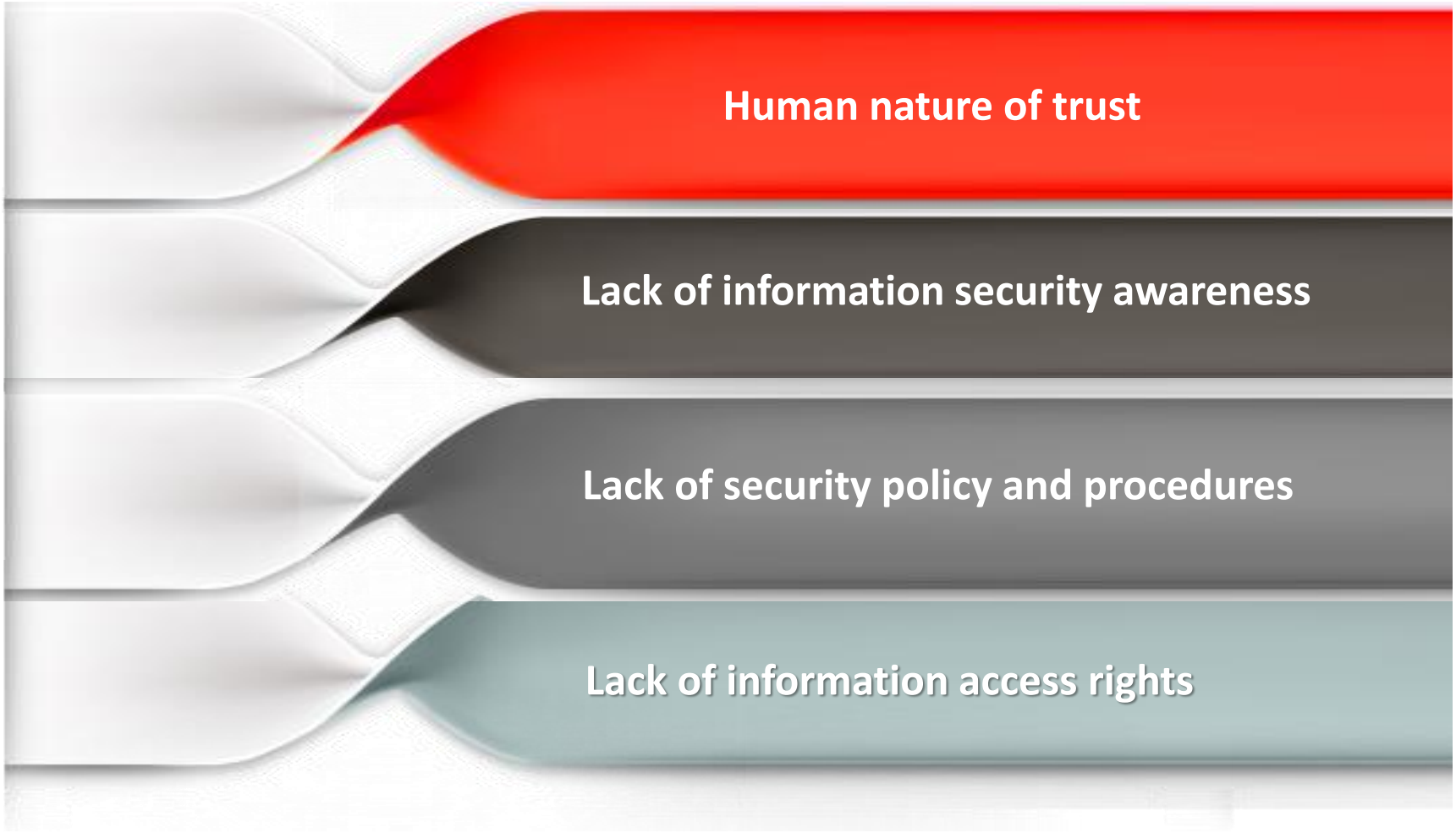
Social Engineering is the art of manipulating people into performing actions that lead to breach of confidential data & give access to personal sensitive information.



What are they searching for?

- Collect sensitive information
- Identity theft
- Targeted attacks

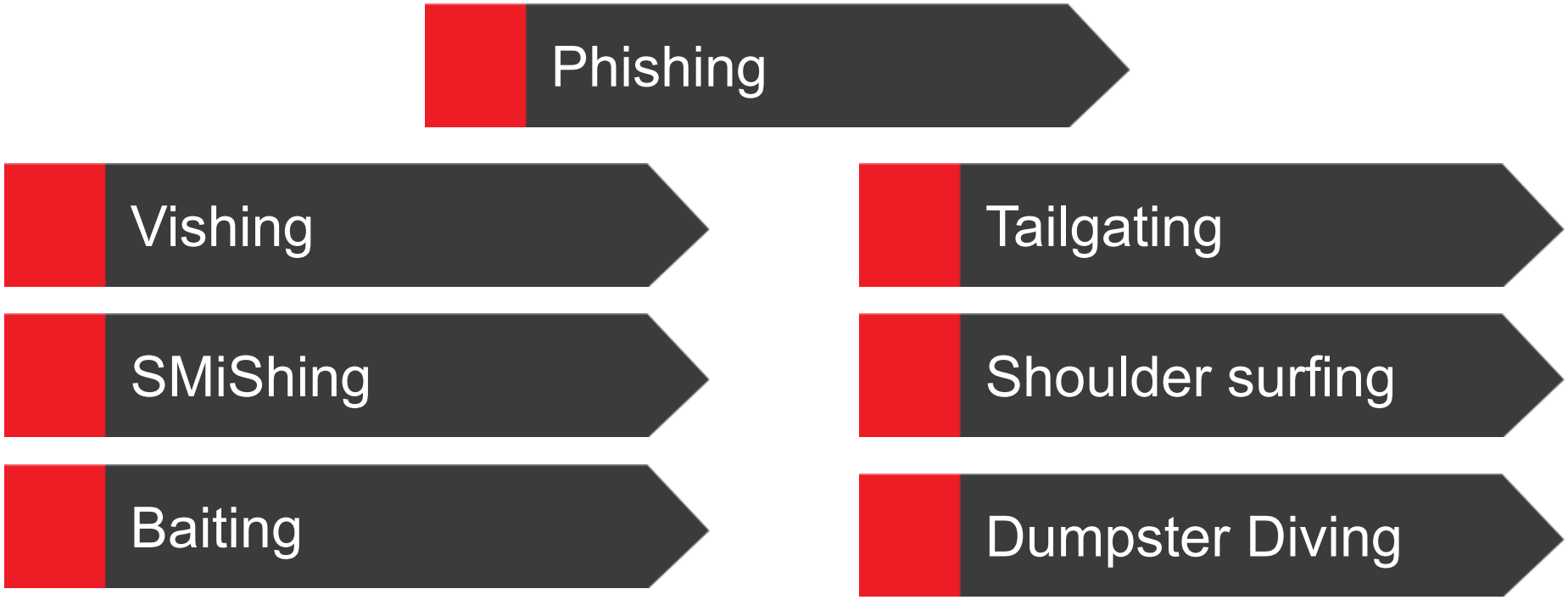
Why they Succeed?



Social Engineering

Techniques

Techniques


Phishing
Vishing
SMiShing
Baiting
Tailgating
Shoulder surfing
Dumpster Diving

Social Engineering

Phishing

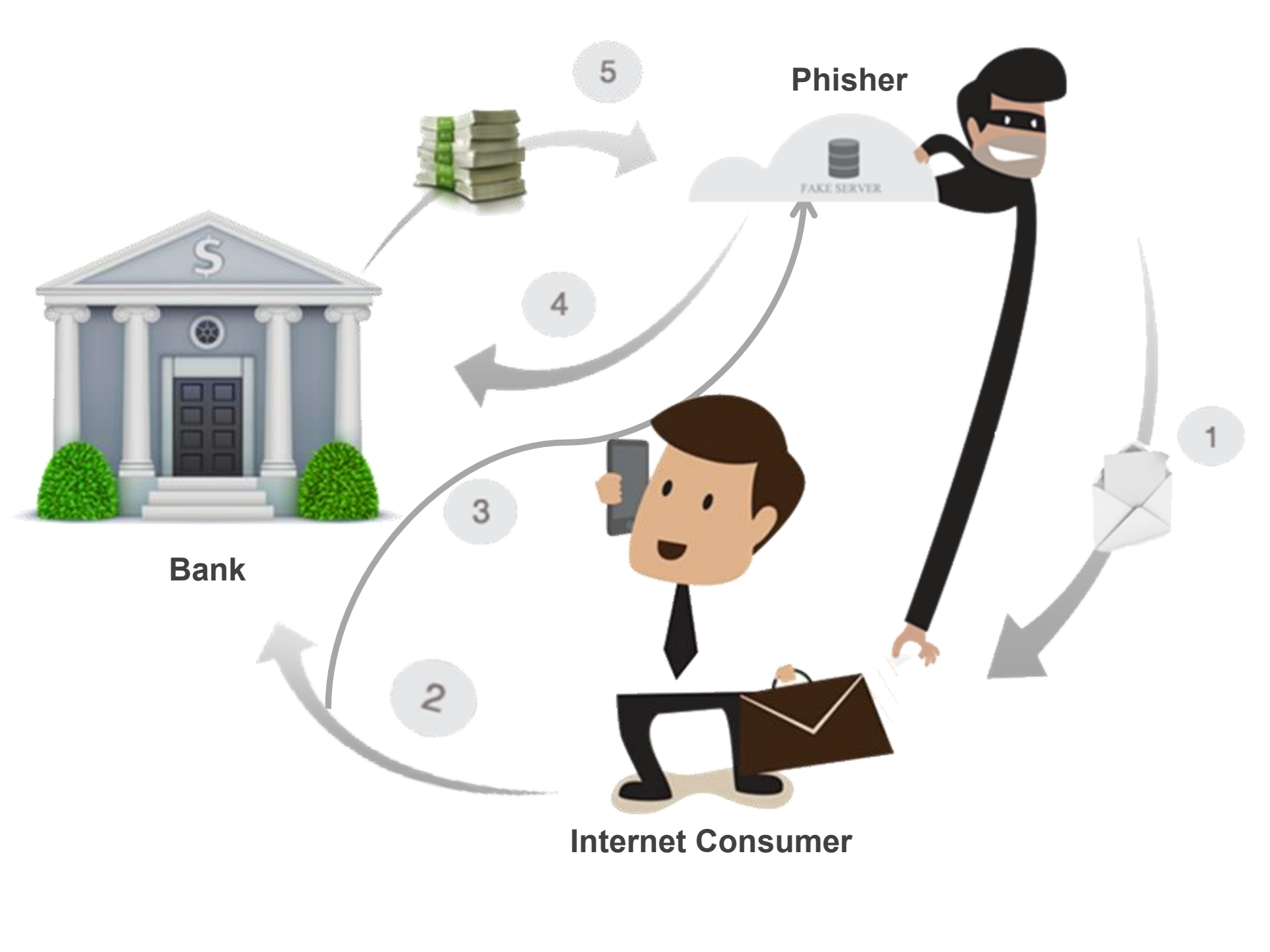
Phishing

It is a kind of email fraud where the fraudster sends out a legitimate looking email posing as a trusted entity which is designed to extract sensitive information.

Did You Know?

94% of malware is delivered via email

Source: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html


5
Phisher
FAKE SERVER
4
1
3
Bank
2
Internet Consumer

Phishing: General Phishing

What is it?
Email messages claiming to come from trusted sources like your bank asking you to verify your account, re-enter your personal information or make a payment.

Why?
To trick you into providing your bank account details in order to access your bank account then steal your money

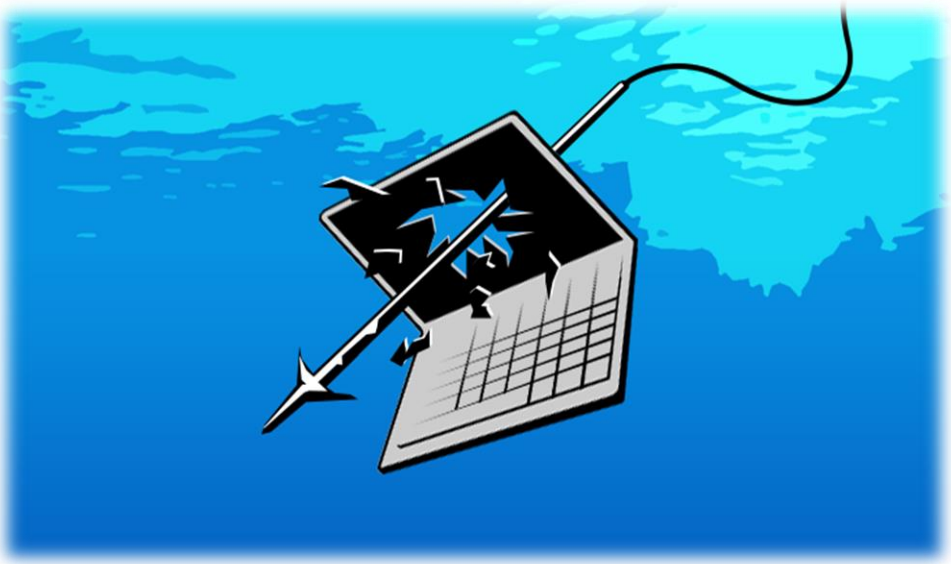
How to Avoid?
Compare these messages with ones you already have and call the source to re-verify

Phishing: Spear Phishing

What is it?
Email messages usually targeting higher profile people who have valuable information

Why?
Directly targeting you to access your bank account then steal your money or collect sensitive information

How to Avoid?
Look out for spelling mistakes and fake URLs



Phishing: Authority Fraud

What is it?
Email messages with addresses similar to that of an authority to request confidential information or request payments within the country.

Why?
To trick the victim to provide confidential information or transfer money to the cybercriminals

How to Avoid?
Double-check suspicious requests with the authority before providing information or sending money

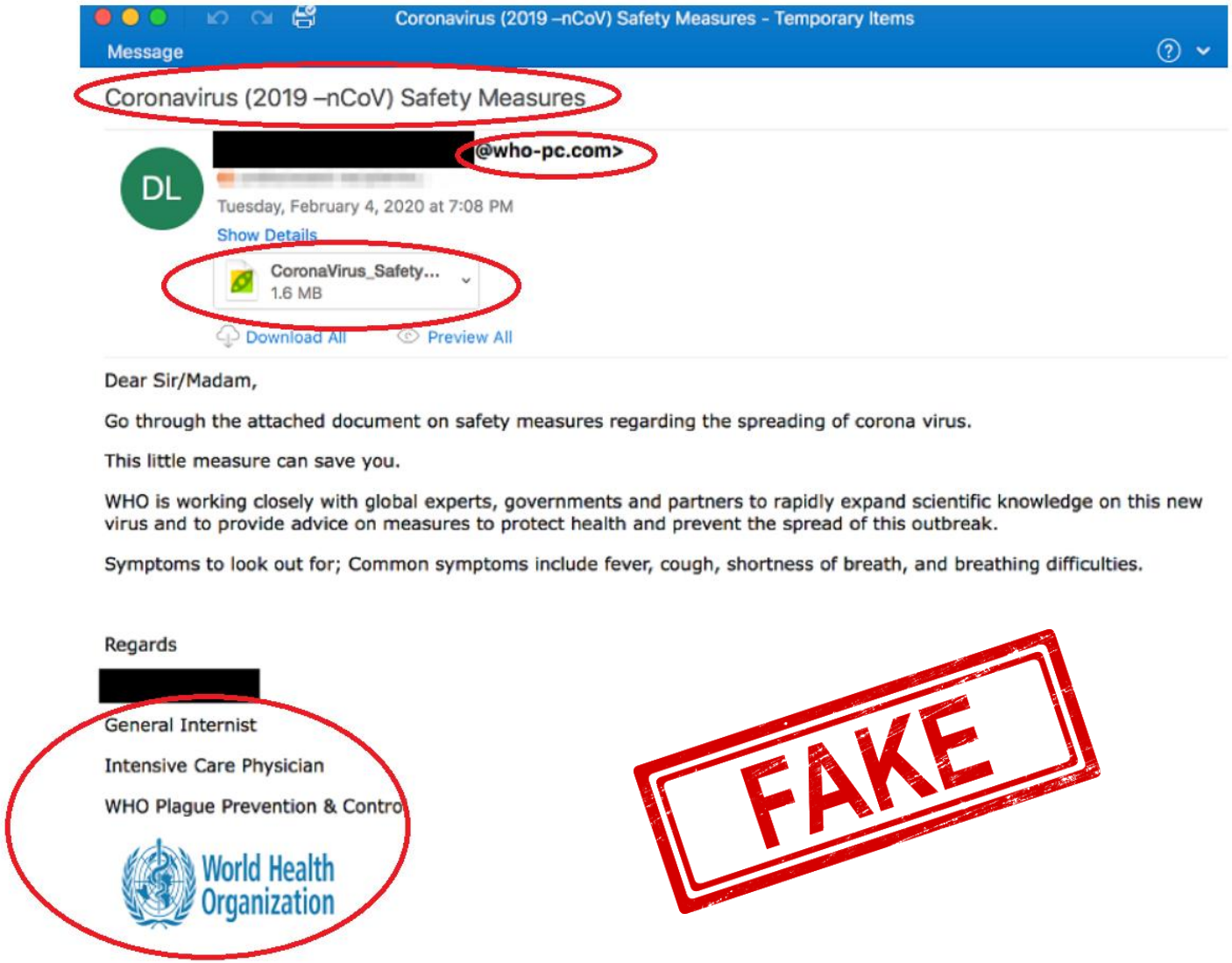
Phishing: Pharming

What is it?
Redirecting website traffic through hacking which may cause users to find themselves on an illegitimate website without realizing they have been redirected to an impostor site, which may look exactly like the real site.

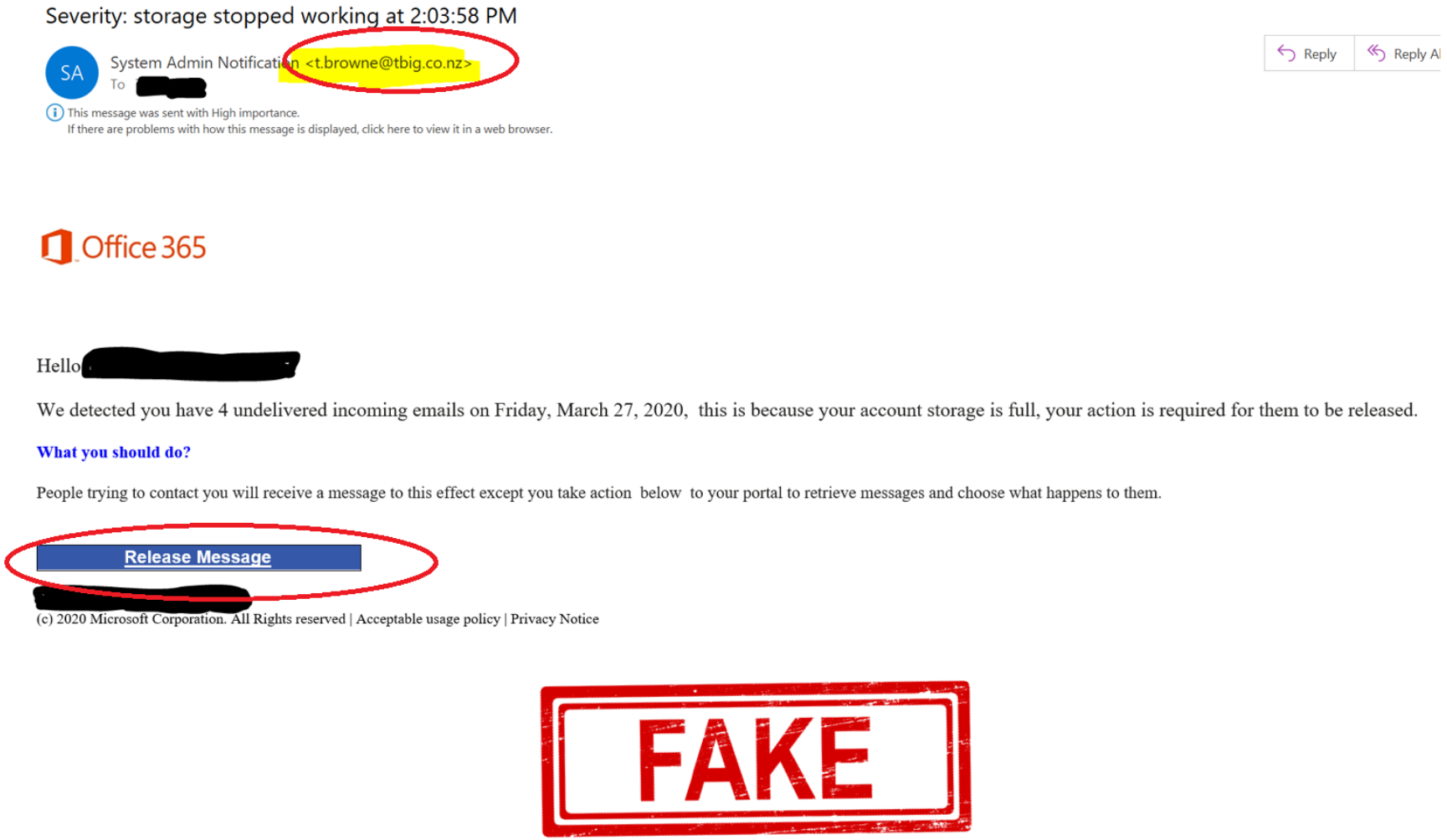
Why?
To intercept and steal sensitive information or online payments

How to Avoid?
Check the URL and look for secure certificate

Phishing: Examples
Fake Email Messages



Phishing: Examples
Fake Email Messages



Severity: storage stopped working at 2:03:58 PM

SA System Admin Notification <t.browne@tbig.co.nz>
To [redacted]

Reply | Reply Al

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Office 365

Hello [redacted]

We detected you have 4 undelivered incoming emails on Friday, March 27, 2020, this is because your account storage is full, your action is required for them to be released.

What you should do?

People trying to contact you will receive a message to this effect except you take action below to your portal to retrieve messages and choose what happens to them.

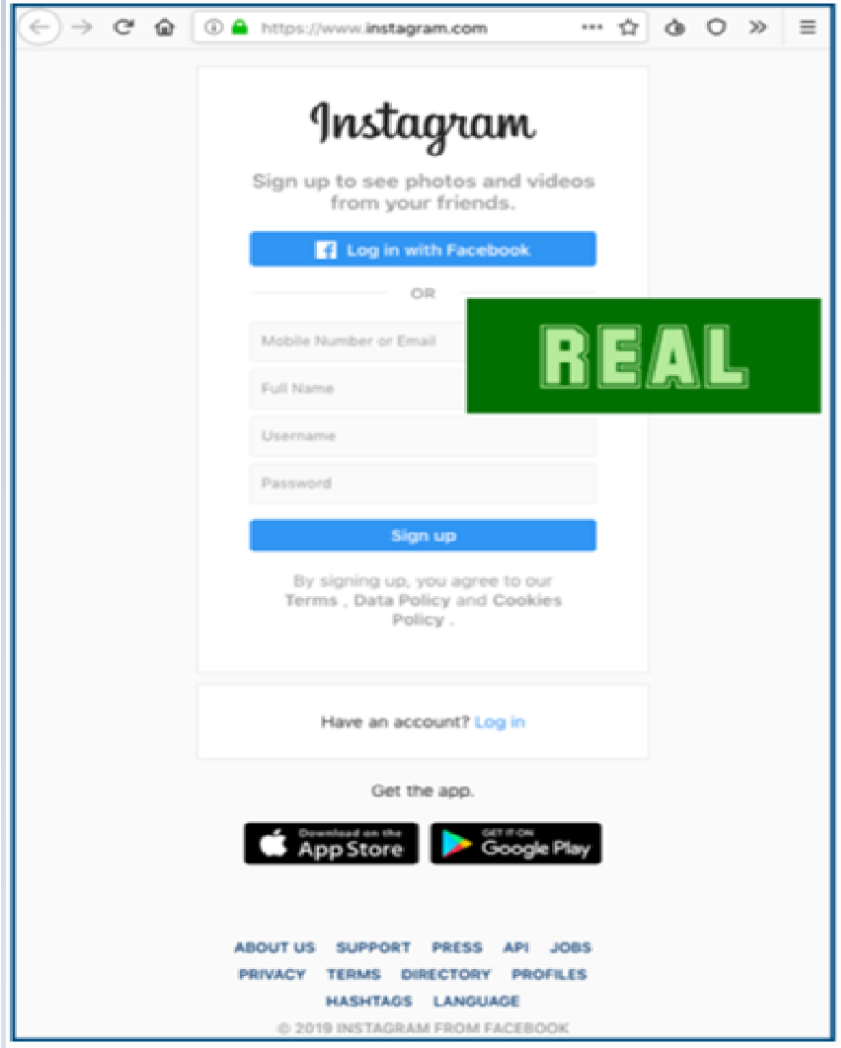
Release Message

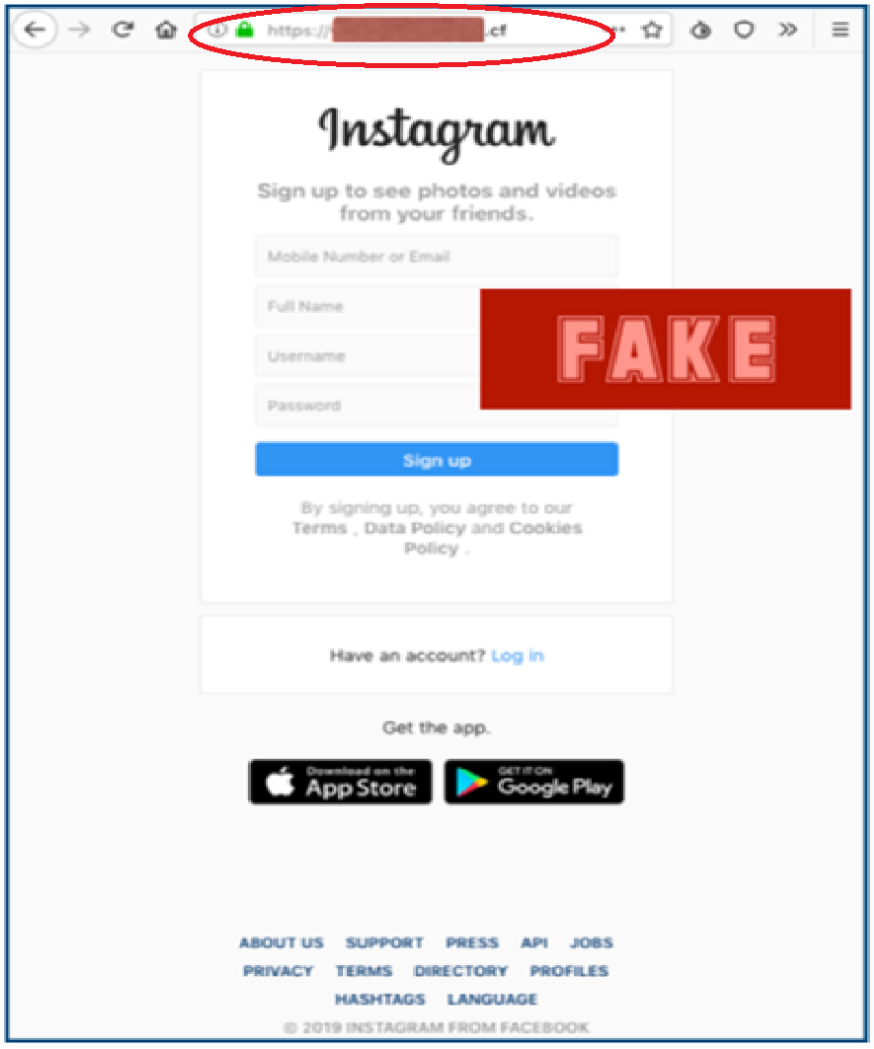
[redacted]

(c) 2020 Microsoft Corporation. All Rights reserved | Acceptable usage policy | Privacy Notice

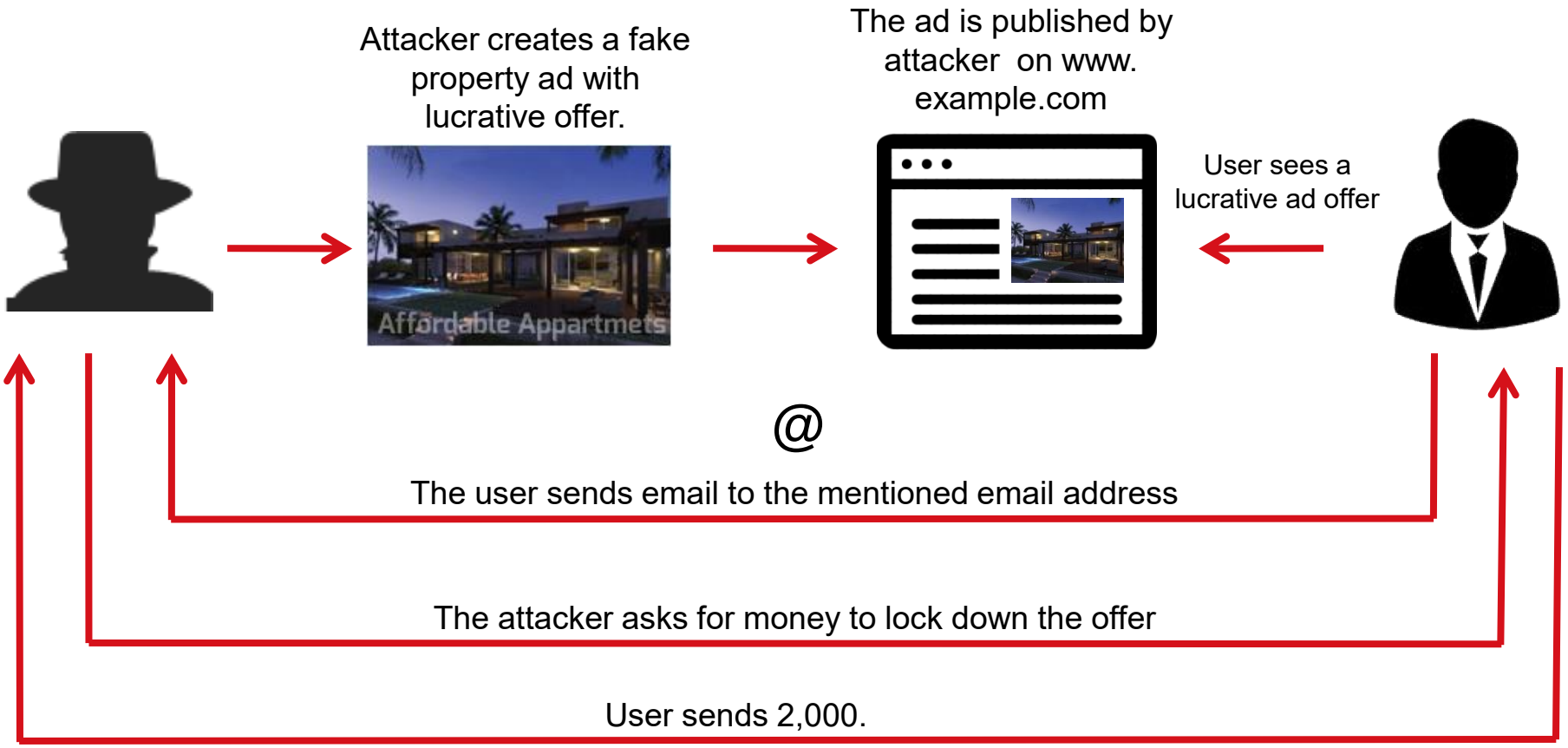
FAKE

Phishing: Examples
Fake Websites





Example Scam



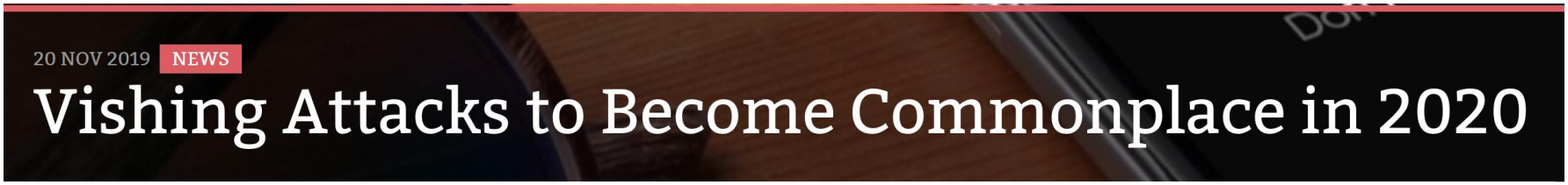
Social Engineering

Vishing

Vishing

Collecting sensitive information or attempting to influence action via the telephone. To obtain valuable information that could contribute to the direct compromise of the victim or the organization by exploiting peoples' trust and willingness to help

Vishing news



20 NOV 2019 NEWS

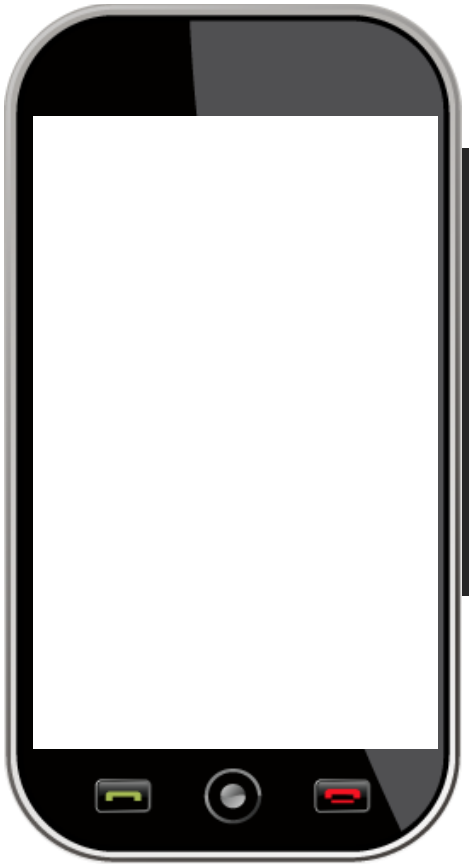
Vishing Attacks to Become Commonplace in 2020

During 2019 to February this year, Abu Dhabi Police arrested 13 criminal gangs made up of 142 fraudsters involved in vishing attacks. The fraudsters were posing as bank employees

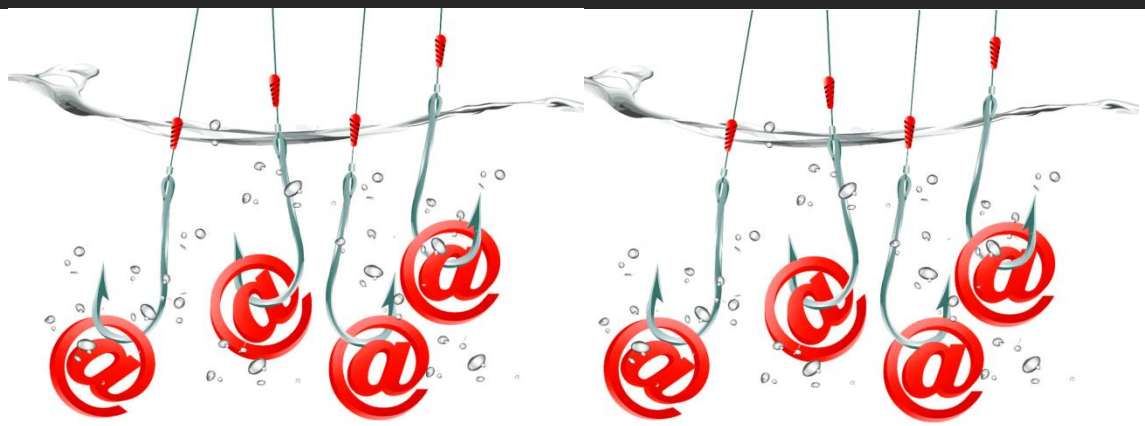
"You cannot find a phishing or vishing news story that does not involve COVID-19," Christopher Hadnagy, chief human hacker at Social-Engineer LLC, told the *Business Journal*.

Source:
https://www.infosecurity-magazine.com/news/vishing-attacks-to-become/
https://gulfnews.com/business/banking/uae-banking-sector-joins-law-enforcement-agencies-to-fight-fraud-1.70971327
https://www.csbj.com/2020/04/10/hackers-exploit-pandemic-to-attack-businesses/

Vishing: Examples
Fake Phone call



"Hello. This is Alex calling from your telecom provider. You have a refund due which I would like to remind you of, but first can you please provide your credit card number for verification before we proceed ? "

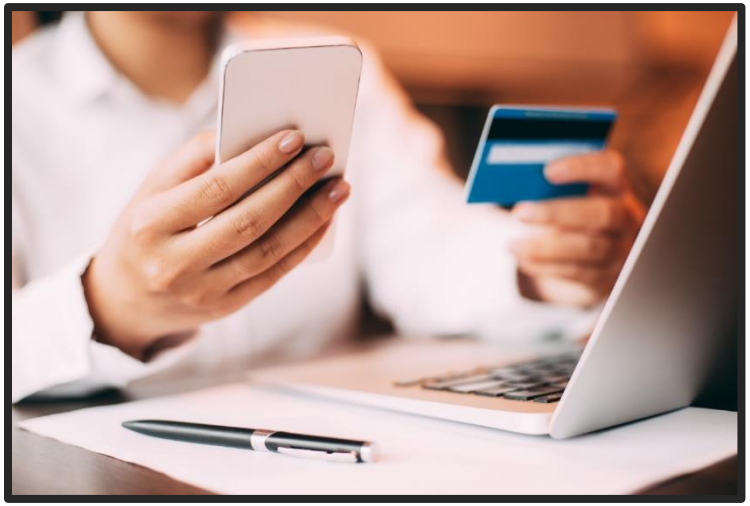


Social Engineering

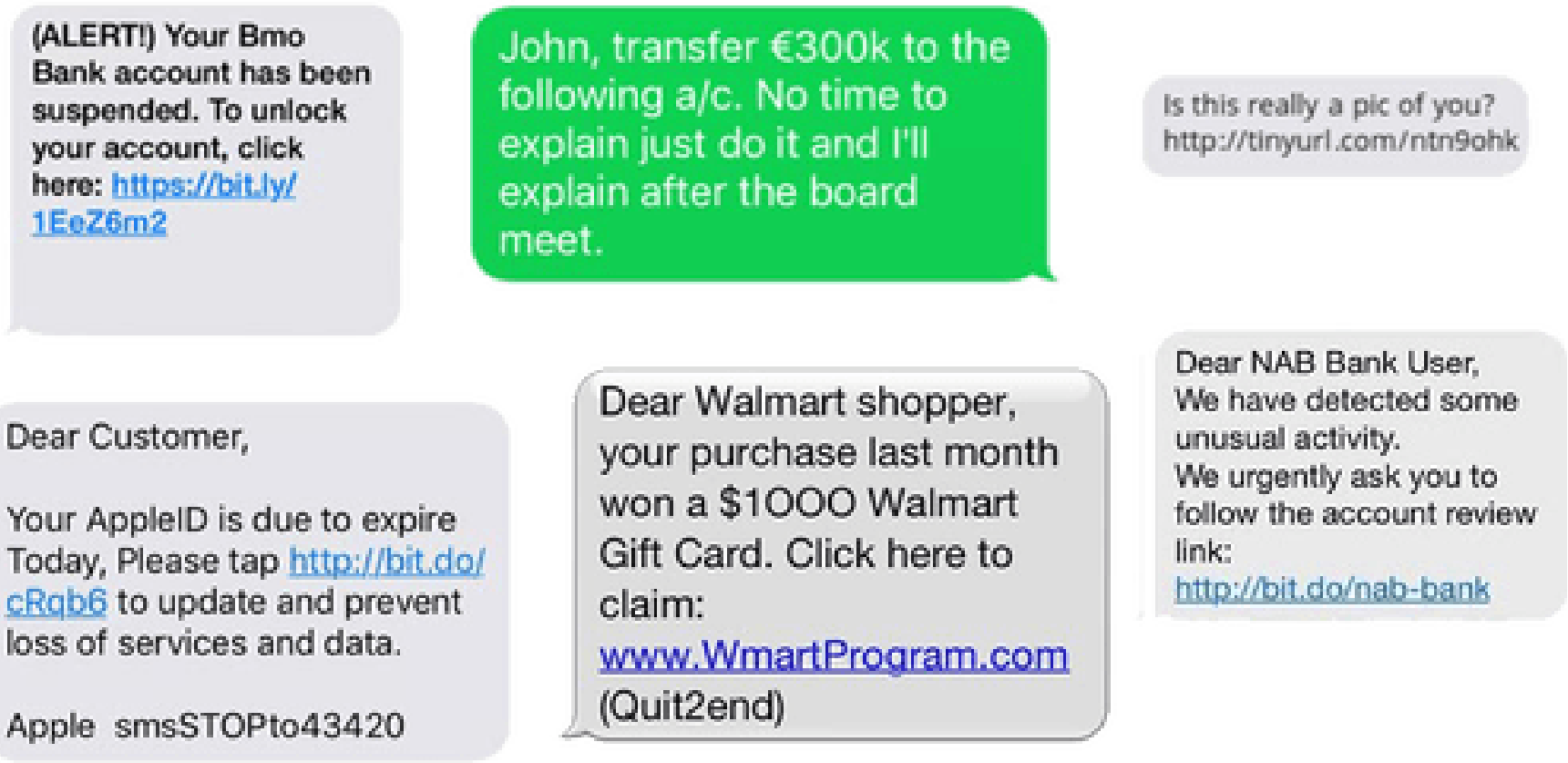
SMiShing

SMiShing

Using mobile phone text messages (SMS) to push victims into immediate action such as downloading mobile malware, visiting a malicious website or calling a fraudulent phone number extract sensitive information or steal money



SMiShing: Examples
Fake SMS



Social Engineering

Baiting

Baiting

With the use of physical media like a USB or a CD, the attacker tries to capture the attention of the victim by giving it a mysterious label and deliberately placing it where it can be easily found (washroom, elevator etc).

Social Engineering

Tailgating

Tailgating

Physically following someone into a limited access area

Could you please open the door? My hands are full..

Social Engineering

Shoulder Surfing

Shoulder Surfing

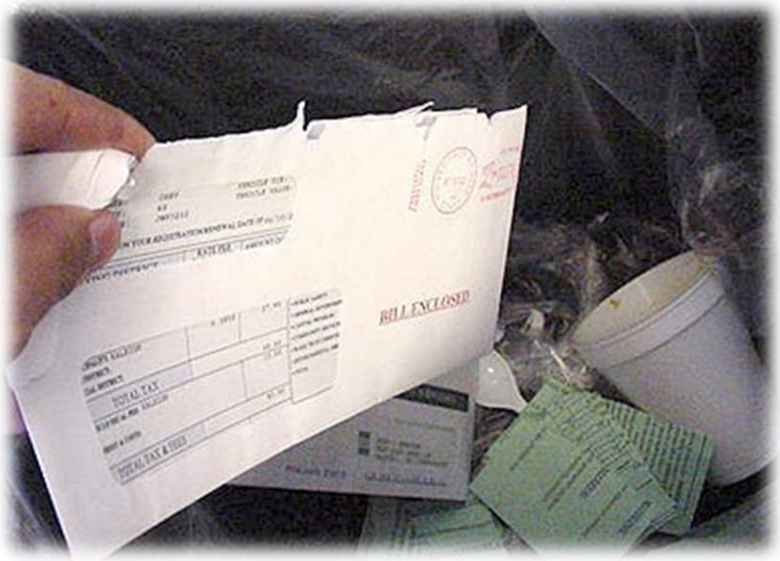
Shoulder surfing is watching someone's login credentials, ID number, POS terminal PIN, ATM PIN or any other personal secret credentials by looking over their shoulder while they are using it.

Social Engineering

Dumpster Diving

Dumpster Diving

It is a method of stealing personal information by digging through a company's dumpster or trash



Login: john
Password: wombat55

Social Engineering

Protect yourself and your organization

Best Practices

01 Information Security Awareness Trainings

02 Establish Policies & Procedures to recognize and respond to social engineering threats

03 Build a security-aware culture

04 Be aware of providing personal information to avoid being a victim of phishing, Vishing or SMiShing attacks

05 If you are an organization, perform unannounced periodic tests of the network

06 Have a proper waste management system to avoid dumpster diving

07 Respectfully refuse to lend your identity token / security pass to avoid tailgaters access the building

08 Do not use a device on your computer unless it belongs to you or is given to you for a purpose from a trustworthy person

09 Review the above steps periodically

Questions


WHAT? HOW? WHEN?
WHO? WHERE? WHO?
WHEN? WHY? WHAT?
WHY? HOW?
WHERE? WHAT? WHO?
HOW? WHERE?
WHO? WHERE? WHO? WHY? HOW?
HOW? WHERE?
WHAT?
WHO?
WHY?
WHY? WHAT?
WHERE?
WHAT? WHEN?
WHERE? WHO?
HOW? WHAT?
WHO? WHERE?
WHY? WHAT? HOW?
HOW? WHO? WHEN?
WHAT? WHERE?
WHY? WHEN? WHAT?
WHERE?
WHO? WHY? HOW?
HOW? WHERE?
WHAT? WHY?
WHEN?
WHO? WHAT?
WHERE? WHAT? HOW?
WHO? WHY? WHERE?
WHAT? WHEN?
WHERE?
WHO? WHAT?
WHERE? WHY?
HOW? WHEN?
WHAT? WHO?
WHEN?
WHY? WHERE?
WHEN? HOW?
HOW? WHERE? WHO? WHAT?
WHY? WHAT? WHEN?
WHERE? HOW?
WHAT?
WHEN? WHO?
WHERE?