Social Engineering

Cybersecurity Awareness
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?

- Human nature of trust
- Lack of information security awareness
- Lack of security policy and procedures
- Lack of information access rights
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

Phisher

Bank

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

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of coronavirus. This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for: Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[Signature]

General Internist
Intensive Care Physician
WHO Plague Prevention & Control

World Health Organization

FAKE
Phishing: Examples
Fake Email Messages

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

To: [redacted]
From: <t.browne@tbig.co.nz> [redacted]

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 [Name],

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

(c) 2020 Microsoft Corporation. All Rights reserved | Acceptable usage policy | Privacy Notice
Phishing: Examples
Fake Websites
Example Scam

Attacker creates a fake property ad with lucrative offer.

The ad is published by attacker on www.example.com

User sees a lucrative ad offer

The user sends email to the mentioned email address

The attacker asks for money to lock down the offer

User sends 2,000.
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

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:
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

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1EeZ6m2

John, transfer €300k to the following a/c. No time to explain just do it and I'll explain after the board meet.

Is this really a pic of you? http://tinyurl.com/ntn9ohk

Dear Customer,
Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.
Apple smsSTOPto43420

Dear Walmart shopper, your purchase last month won a $1000 Walmart Gift Card. Click here to claim:
www.WmartProgram.com
(Quit2end)

Dear NAB Bank User, We have detected some unusual activity. We urgently ask you to follow the account review link:
http://bit.do/nab-bank
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).
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
If you are an organization, perform unannounced periodic tests of the network

Have a proper waste management system to avoid dumpster diving

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

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

Review the above steps periodically
Questions