A GUIIDE::
PROTECTIING YOURSELF FROM SOCIIAL ENGIINEERIING TRIICKS

Presentation By
Jeslyn Ho Ka Yan

EMBARK ON A JOURNEY: UNRAVELING THE MYSTERIES OF SOCIAL ENGINEERING

What is social Engineering?

- the craft of tricking people into disclosing sensitive information or acting in a certain way.

Why is it so dangerous?

- One of the most powerful reconnaissance acts.
- Something beyond the protection of security tools.

It poses a significant threat to everyone.

WHAT SHOULD WE DO?

Cracking the Code:
Exploring the types of Social Engineering Tactics

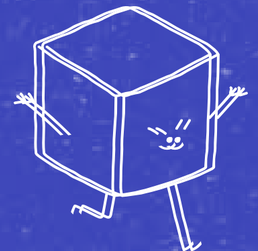
Mind Tricks Games:
Human Psychology behind Social Engineering

Spot the Spy:
Identifying Social Engineering Tactics

Confronting Chaos:
The Impact of Social Engineering Attacks

Armor Up:
Defending Against Social Engineering

Cracking the Code: Exploring the types of Social Engineering Tactics



EXPLORING THE TYPES OF SOCIAL ENGINEERING TACTICS

1. Phishing (most popular type)

- **Definition:** Phasing emails that appear to be from reliable sources in an effort to pressure recipients into sending private information or acting.
- **Examples of Phishing**
  - Phishing Bank Emails: Requests to update account info leading to identity theft.
  - Spoofed Company Emails: Encouraging clicks on harmful links or malware downloads.

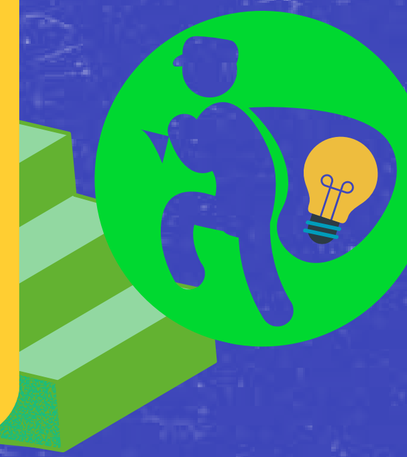
EXPLORING THE TYPES OF SOCIAL ENGINEERING TACTICS

2. Pretexting

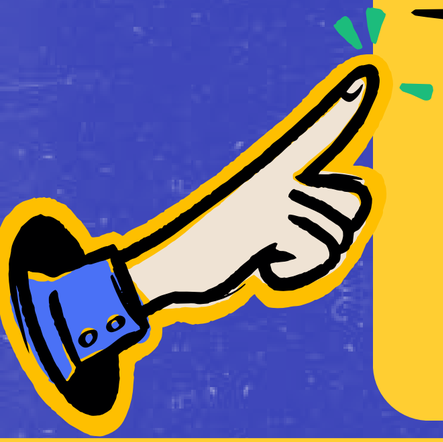
- **Definition:** Crafting elaborate lies to appear legitimate and impersonate a figure to extracting sensitive information.
- **Impersonate :** a trusted figures, your boss, a police officer, debt collectors, etc...

3. Diversion Theft

- **Definition:** Trick victims into sending sensitive data to wrong recipients.
- Spoof reputable email accounts such as those of financial institutions or auditing agencies to trick victims.



EXPLORING THE TYPES OF SOCIAL ENGINEERING TACTICS



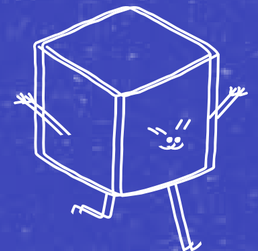
4. Baiting

- **Definition:** provides alluring bait—such as free downloads—to trick people into installing malware or disclosing personal information.
- **Examples:** Offering a fake salary bonus in exchange for personal information

5. Quid Pro Quo

- **Definition**: Utilizes reciprocity desires by offering a reward, such a gift or service, in return for personal information or activities.
- **Examples**: Offering free gaming coins/skins in exchange for your account login information. It's a trap!

Mind Tricks Games: Human Psychology behind Social Engineering



HUMAN PSYCHOLOGY BEHIND SOCIAL ENGINEERING

RECIPROCATION:

Human tends to feel compelled to repay someone for a favor, which allows the attacker to take advantage of it.

Example

Victim posts personal information on social media to repay a favor.

SCARCITY:

taking advantage of the fear of losing out on chances or scarce resources.

Example:

Threatening limited tickets to a Taylor Swift concert in Singapore, leading to impulsive purchases.

CONSISTENCY:

People usually follow through on their promises and get used to routines.

Example:

Hackers mimic the identity of reputable suppliers, taking advantage of trust to distribute devices compromised with malware.

HUMAN PSYCHOLOGY BEHIND SOCIAL ENGINEERING

LIKING :
Compliance increases when requests come from liked or attractive individuals.

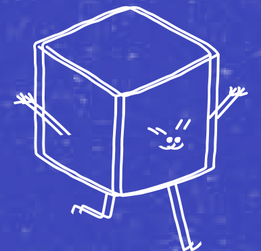
AUTHORITY:
Leverages obedience to figures of authority.

Example:
Victims comply with orders to provide private information to a person assuming the role of an authority.

VALIDATION::
Copying others, so that they will not feel out of place

Example:
Fearing social rejection, victims acquiesce to demands if they observe others doing the same.

Spot the Spy: Identifying Social Engineering Tactics

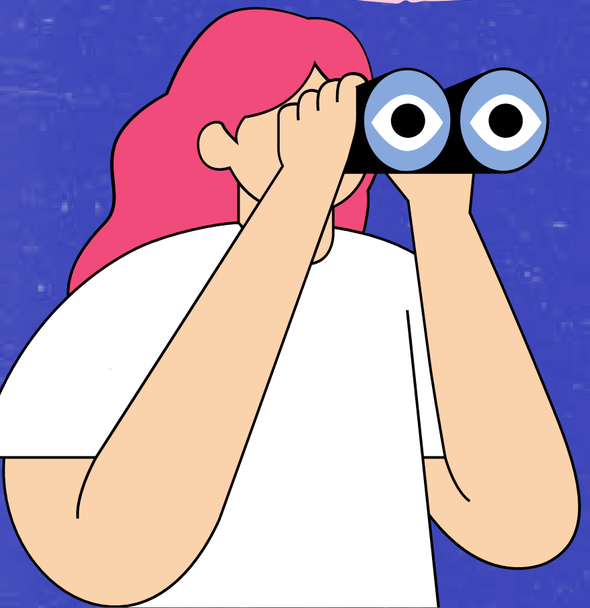


SPOT THE SPY: IDENTIFYING SOCIAL ENGINEERING TACTICS

IDENTIFYING PHISHING ATTACKS

HOW TO IDENTIFY ANOMALIES

SOCIAL ENGINEERING RED FLAGS



IDENTIFYING PHISHING ATTACKS

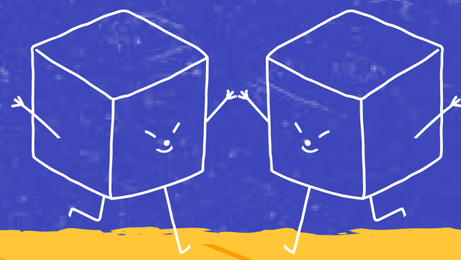
- **Suspicious Sender**: Look for anomalies or strange characters in the sender's email address.
- **Sense of Urgency:** Watch out for emails that demand quick action, such ones that threaten to suspend your account or include time-limited deals.
- **Unsolicited Requests:** Be wary of unsolicited requests, particularly if they purport to be from respectable organisations, for money or personal information.

- **Links & Attachments:** Steer clear of clicking on links or downloading attachments from strange or dubious emails, as they could take you to phishing websites or contain malware.
- **Grammatical errors:** Since official organisations usually use professional communications, be on the lookout for spelling and grammar errors.

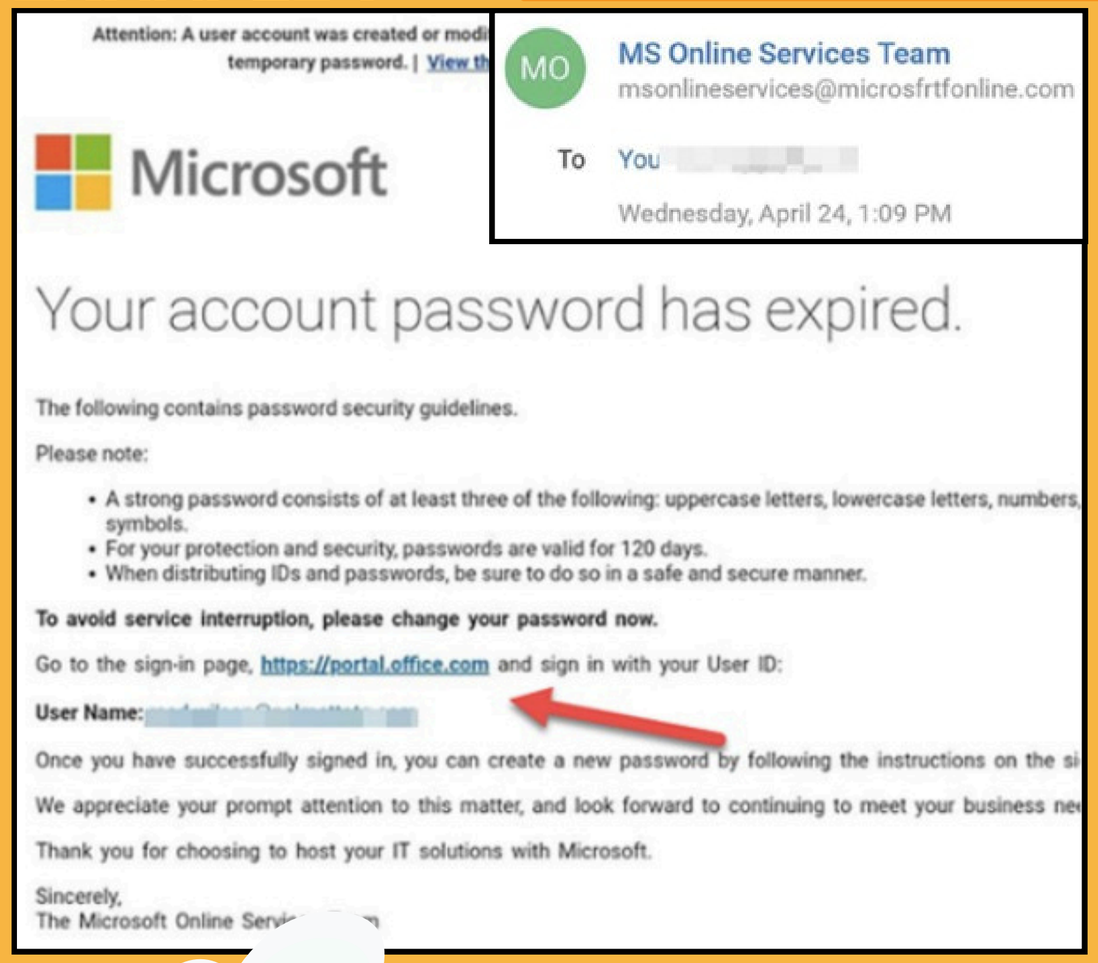
TESTING YOUR AWARENESS

WHICH ONE IS NOT A PHISHING ATTACKS ?

LET'S PLAY!



EXMAPLE 1



Attention: A user account was created or modi
temporary password. | View th

Microsoft

MO

MS Online Services Team
msonlineservices@microsfrtfonline.com

To You

Wednesday, April 24, 1:09 PM

Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, symbols.
- For your protection and security, passwords are valid for 120 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page, https://portal.office.com and sign in with your User ID:

User Name:

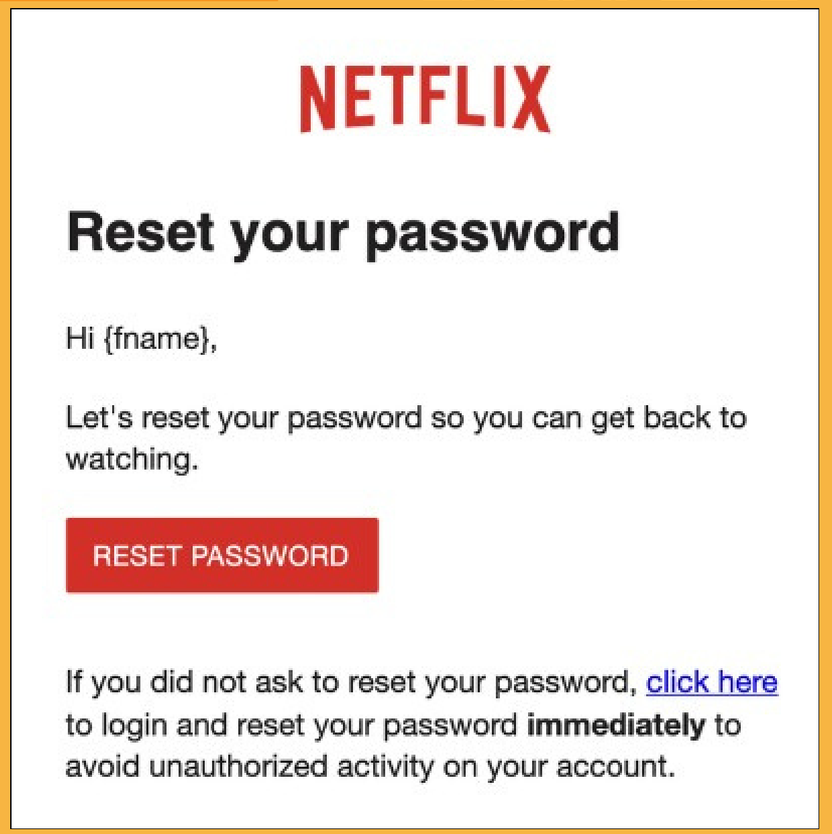
Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business ne

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Servi

EXMAPLE 2



NETFLIX

Reset your password

Hi {fname},

Let's reset your password so you can get back to watching.

RESET PASSWORD

If you did not ask to reset your password, click here to login and reset your password **immediately** to avoid unauthorized activity on your account.

EXMAPLE 3

Chase Online Alert

RS

Rackspace Support <217376@inha.ac.kr>
To me

Dear Customer,

At rackspace, we're committed to providing the tools you need to help you monitor your account(s).

*A review of your recent activities regarding multiple login attempt has raised some concern.

For your safety we have suspend your login access.Some or all of your emails may have been deleted.

Use the link below to remove restriction on yo

https://www.thefitdollar.com/gabbyr/ftimer.html
Click or tap to follow link.

https://app.rackspace.com/remove/restriction/access

Please do not reply to this Automatic Alert.

We appreciate your business.

Sincerely,

Online Email Team

EXMAPLE 4

SD

Tue 3/12/2019 3:35 PM

Shona Dyck <tmpmustang@cox.net>

Regarding Job

To

Shona Dyck Resume.doc
37 KB

How are you doing?
My name is Shona Dyck and I'm interested in a job.

I've attached a copy of my CV.
The password for the document is 1234

Thank you!

--
Shona Dyck

EXMAPLE 5

From: Account Support <reza.clalucyankdia6@gmail.com>
Sent: Monday, February 15, 2021 6:41:04 AM
To: [redacted]
Subject: Re: Your account has been filtered by our system for authentication.

PayPal

Dear Customer,

Your account has been filtered by our system for authentication. Please view the possible events listed below for this cause.

Possible events occurred

1. Log in attempts from, Windows 7 - Ontario, Canada.
2. Requesting any operation using unusual pattern.
3. Too many incorrect log in attempts.

For security, all your account features are disabled until a response has been received from you.

Please click "Authenticate now" button below to secure your account.

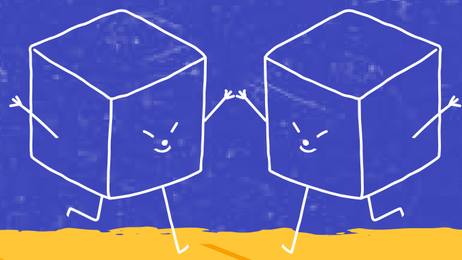
Authenticate now

Best regards,

PayPal Inc Help Center

Answer

ALL OF THEM ARE PHISHING ATTACKS

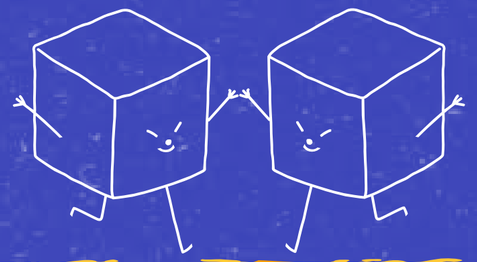


TESTING YOUR AWARENESS

EXAMPLE 1

THE DOMAIN NAME IS MISSPELT

- Misspelled domain names can be created due to registrars selling domains to anyone.
- Similar addresses can be constructed, despite each domain needing to be unique.



Attention: A user account was created
temporary password. |

Microsoft

MO

MS Online Services Team
msonlineservices@microsfrtfonline.com

To You

Wednesday, April 24, 1:09 PM

Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, symbols.
- For your protection and security, passwords are valid for 120 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page, https://portal.office.com and sign in with your User ID:

User Name:

Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business ne

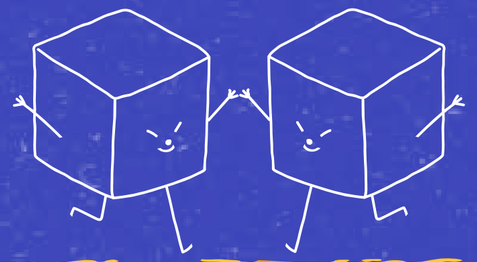
Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team

TESTING YOUR AWARENESS

EXAMPLE 2 SUSPICIOUS LINK

- Legitimate link should direct you to a website address that begins with "netflix.com"
- Beware hidden website addresses!
- Scam emails often use buttons instead of showing the link, making it tricky to see where you'd land.



NETFLIX

Reset your password

Hi {fname},

Let's reset your password so you can get back to watching.

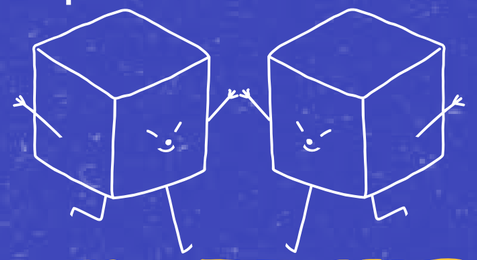
RESET PASSWORD

If you did not ask to reset your password, click here to login and reset your password **immediately** to avoid unauthorized activity on your account.

TESTING YOUR AWARENESS

EXAMPLE 3 (POORLY WRITTEN EMAIL)

- According to the sender's display name, it is signed by the single "Online Email Team" and comes from Rackspace Support.
- "Dear Customer" is a red flag! Real companies likely know your name.
- Multiple grammatical errors and poor capitalization.



Chase Online Alert

RS Rackspace Support <217376@inha.ac.kr>
To me

Dear Customer,

At rackspace, we're committed to providing the tools you need to help you monitor your account(s).

*A review of your recent activities regarding multiple login attempt has raised some concern.

For your safety we have suspend your login access.Some or all of your emails may have been deleted.

Use the link below to remove restriction on yo

https://www.thefitdollar.com/gabbyr/ftimer.html
Click or tap to follow link.

https://app.rackspace.com/remove/restriction/access

Please do not reply to this Automatic Alert.

We appreciate your business.

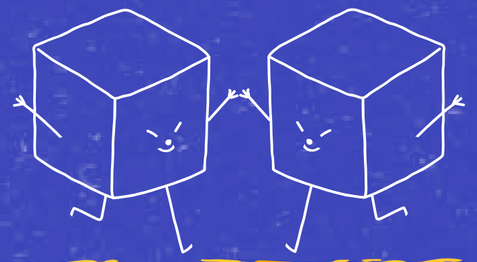
Sincerely,

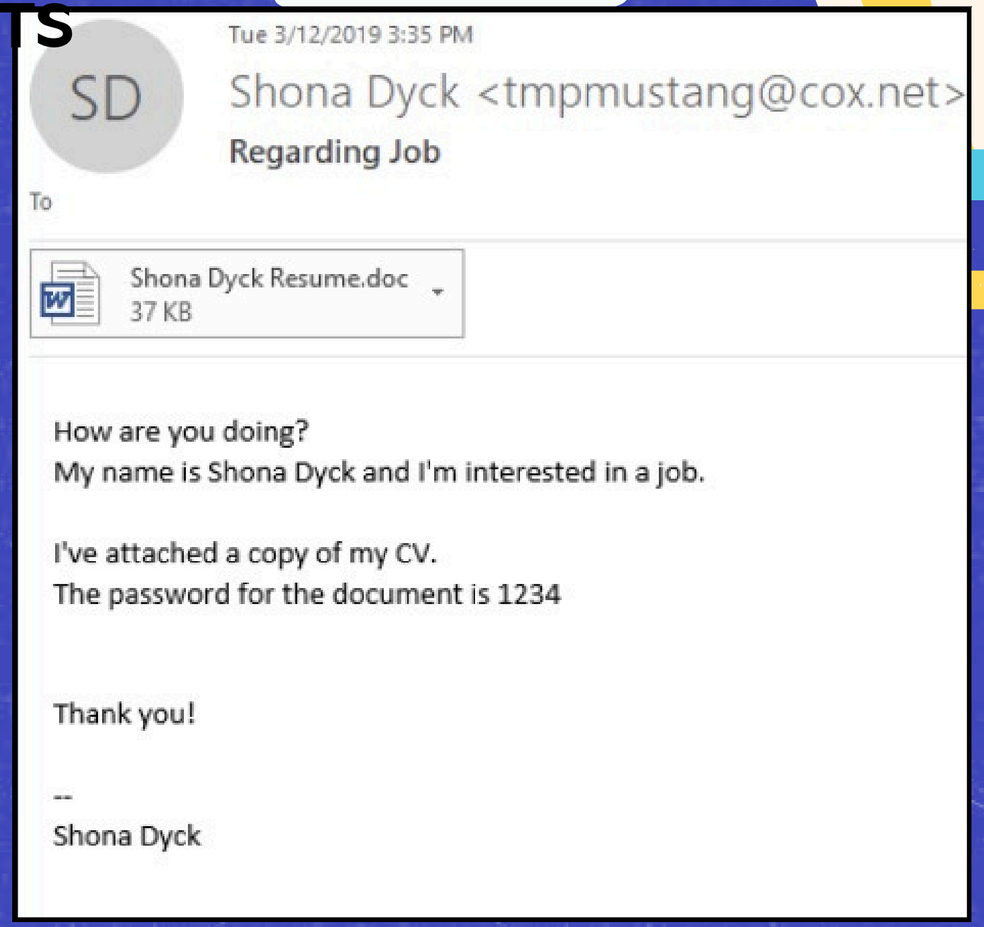
Online Email Team

TESTING YOUR AWARENESS

EXAMPLE 4 INFECTED ATTACHMENTS

- The sender's name would quickly give this away if you were ever a middle school guy, or if you had just spent time near one.



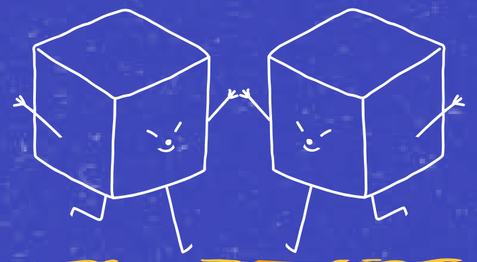


TESTING YOUR AWARENESS

EXAMPLE 5

From: Account Support <reza.clalucyankdia6@gmail.com>
Sent: Monday, February 15, 2021 6:41:04 AM
To: [redacted]
Subject: Re: Your account has been filtered by our system for authentication.

- No legitimate organisation will send emails from
- an address that ends ‘@gmail.com’.



PayPal

Dear Customer,

Your account has been filtered by our system for authentication. Please view the possible events listed below for this cause.

Possible events occurred

1. Log in attempts from, Windows 7 - Ontario, Canada.
2. Requesting any operation using unusual pattern.
3. Too many incorrect log in attempts.

For security, all your account features are disabled until a response has been received from you.

Please click "Authenticate now" button below to secure your account.

Authenticate now

Best regards,

PayPal Inc Help Center

HOW TO IDENTIFY ANOMALIES

Recognizing Unusual Activity

- **Unrecognised Logins:** Keep an eye out for strange or repeated unsuccessful login attempts.
- **Unexpected System Behaviour:** Take note of any abrupt crashes, slowdowns, or configuration changes.
- **Unusual Network Traffic:** Keep an eye out for connections to dubious sites or sudden increases in data use.
- **Abnormal User Behaviour:** Spot anomalies such as downloading a lot of data or viewing strange files.

(Story 1)

Answer

IF you had choose

Option A: Your Financial, Identity and Privacy will be compromise

Option B: Reduce unauthorized access and potential financial loss, identity theft, and privacy breaches.

Option C: Receive guidance from Customer Support. Eg: resetting password or even turning on extra security measures.

(Story 2)

Jeslyn, who works as an IT administrator for a big company, discovers strange behaviour on one of the users' accounts. Yuth, the user, usually only accesses a few files a day, but Jeslyn downloads late at night when Yuth is not usually online, and she observes an abrupt increase in file access.

What should Jeslyn do?

A. Brush it off as a passing anomaly and ignore the strange activity.

B. Investigate Yuth's recent activities and reach out to him directly for further inquiry.

C. Suspend Yuth's account and alert the security team for investigation.

(Story 2)

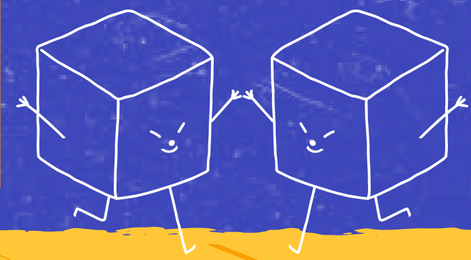
Answer

IF you had choose

Option A: Avoid causing unnecessary alarm or disruption to Yuth's work, but could lead to an undetected data loss or security breach.

Option B: investigate the unusual behavior and address them, but If the action is harmless, reaching out to Yuth directly runs the risk of alerting them unnecessarily.

Option C: Potential threats are addressed by suspending Yuth's account and notifying the security staff, although if the activity is benign, it might interfere with Yuth's work.

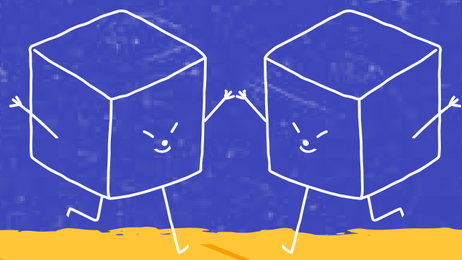


HOW TO IDENTIFY ANOMALIES

- **Unannounced Requests:** Exercise caution while responding to unexpected requests for private information or access.
- **Emotional Manipulation:** Identifying attempts to manipulate someone by inciting fear, urgency, or pity.
- **Recognising abnormal or irregular behaviour**
- **Offers that appear excessively favourable.**

Social Engineering Case Study

LET'S PLAY!



A social engineering attack causes a data leak at a financial institution. Through the use of a false identity and intimidation to get login credentials, the attacker was able to obtain sensitive customer data.

How was the social engineering attack carried out by the attacker using human imperfections?

In order to identify and stop the attack, what could the financial institution have done differently?

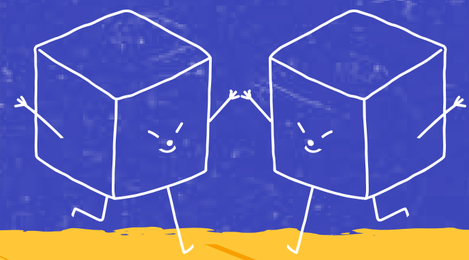
Answer

How was the social engineering attack carried out by the attacker using human imperfections?

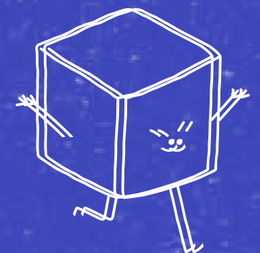
- Impersonated a trusted employee to gain credibility.
- Utilised authority or urgency to pressure employees into disclosing private information.

In order to identify and stop the attack, what could the financial institution have done differently?

- In order to confirm user identities, multi-factor authentication was used.
- Regularly held security awareness training sessions to inform staff members about social engineering techniques.



Confronting Chaos: The Impact of Social Engineering Attacks



The Impact of Social Engineering Attacks

Financial Loss : Scams, fraudulent schemes, or unauthorised access to accounts can cause victims to lose money.

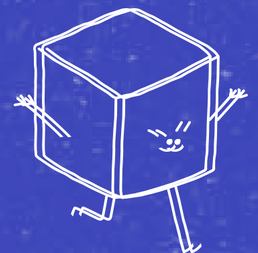
Identity Theft: When personal information is stolen, it may be used illegally or inappropriately.

Emotional Distress: Stress and shame are frequent experiences for victims.

Reputation damage: When there is a breach of trust, people or organisations may suffer.

Disruption of Operation: Penalties or fines may be imposed for violation.

Armor Up:
Defending Against Social Engineering



Defending Against Social Engineering

1. Attend a security awareness course
2. Use multi-factor authentication and other robust authentication techniques.
3. Exercise caution when disclosing information.
4. Continually patch and update software, and make data backups.
5. Make secure and distinctive passwords:
6. Watch out for shady phone calls and emails:
7. Advising friends, family, and coworkers to exercise caution

(Build a Security Culture)

Still Unsure after Today’s Guide?

visit

- Cybrary: Free online courses on cyber security that address defence tactics and social engineering.
- Krebs on Security: Blog by cybersecurity specialist Brian Krebs, offering analysis and advice on cyber threats.
- OWASP: offers web application security information, tools, and best practices, along with advice on reducing the risk of social engineering during the development and implementation of software.


THANK
YOU