# Take time to think before you click

**We live in an everchanging world of technology. With the surge in internet usage, users are most vulnerable to social engineering attacks. These attacks rely heavily on human interaction and often involve manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks, or physical locations. The reasons for these attacks are for obtaining private information such as trade secrets for personal or financial gain, for sabotage and for corporate espionage.**

**Phishing is an example of a social engineering attack frequently used to steal private information such as login credentials and credit card numbers. It involves receiving emails or text messages containing links which look genuine. The links can be used to direct the user to fake websites, install malware on the computer, freeze a system for ransomware and divulge private information.**

**Attackers can use the following types of phishing:**

## 1. Vishing

Vishing is the deceitful practice of making phone calls pretending to be from reputable companies to entice individuals to reveal personal information such as bank details and credit card numbers. Fraudsters pretend to call from a bank which the user is registered with to get personal data. To avoid vishing attacks, it is encouraged not to answer calls from private or unknown phone numbers and to desist from giving private information over the phone.

## 2. Smishing

Smishing involves receiving a text message / SMS which contains malicious links to get private or personal information. It is important to verify the authenticity of the message before replying or clicking on the malicious link.

## 3. Spear Phishing

Spear Phishing is an attack that targets a certain individual and trick him or her into clicking on malicious links or email attachments so that he or she can provide private information. Fraudsters can also identify their targets by gathering information from social media sites. Users or employees with confidential data are usually a target. It is important to avoid sharing personal, corporate information or any clues of personal information on social media.

## 5. Whaling

Whaling is an attack like spear phishing which targets executives of organizations stealing their login credentials. Fraudsters can commit CEO Fraud which involves using the email account of the CEO or executives to authorize financial transactions via emails.

## Consequences of phishing attacks

Phishing attacks can have the following consequences to both individuals and organizations :

- Funds being stolen from bank accounts
- Use of credit cards to perform unauthorized transactions
- Corporate funds being stolen
- Exposure of private information such as banking details
- Damage to company reputation

## Before clicking any link, one should do the following to avoid being scammed:

## 1. Do not share private information

Avoid sharing your private information such as username, password, and other personal information especially via email, phone and text message. No genuine organization will request for your private information via email, phone, and text message

## 2.Be cautious of all email attachments and links

Do not think that every email is genuine. Email attachments and links are frequently used to send malicious software. Verify all email attachments and links before opening. Malicious emails usually contain spelling errors, grammatical mistakes and generic salutations.

## 3.Establish the truth about the sender of the email

Fraudsters use organizations or companies' identities to appear authentic. They use email addresses, symbols, signatures and logos that resemble the original organization or company. Verify the email address before clicking on the link or sending a reply.

## 4. Do not act hastily

Most messages sent out by fraudsters usually want users to react with fear and urgency by giving a particular condition such as a link expiring in a short period of time. Users must not conform to such conditions as these messages are usually fake.

One important thing to do to avoid being scammed is to **take time to think before you click. Fraudsters are just waiting for that one click from a user.**