Phishing

October 5, 2020
In News

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone **posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.** The information is then used to access important accounts and can result in **identity theft and financial loss.**

Phishing is the simplest kind of cyberattack and, at the same time, the most dangerous and effective. That is because it attacks the most vulnerable and powerful computer on the planet: the human mind. **Phishers are not trying to exploit a technical vulnerability in the device's operation system, they're rather using social engineering.**

Features of Phishing Emails

- **Too good to be true** – Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize.
- **Sense of urgency** – A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond.
- **Hyperlinks** – A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling,

- **Attachments** – Attachments in an email often contain payloads like ransomware or other viruses.

Means to Prevent Phishing

- To protect against spam mails, **spam filters** can be used. Generally, the filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it's spam.
- The **browser settings** should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked or an alert message is shown.
- Another way to ensure security is to change passwords on a regular basis, and **never use the same password for multiple accounts.**
- Banks and financial organizations use monitoring systems to prevent phishing. Individuals can report phishing to industry groups where **legal actions can be taken against these fraudulent websites.**
- If there is a link in an email, hover over the URL first. **Secure websites with a valid Secure Socket Layer (SSL) certificate begin with "https".**