

India is currently third in the world to witness the maximum number of cyber attacks. Lack of awareness and understanding of cyber risks have led to the surge in online frauds, scams and data breaches.

India Post Payments Bank is committed to the safety of its customers accounts and as such the banking safety & awareness series is launched aimed at educating the patrons of the various cyber threats around so that fraudsters can be kept at bay.

Phishing



Phishing is a type of social engineering attack where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software (ransomware) on the victim's infrastructure.

As of 2020 Phishing is by far the most common attack performed by cyber criminals and it has been on the rise. Per Sequeretek, a Mumbai based security firm, India has seen a whopping 4000% spike in phishing emails in 2020.

Some of the significant forms of Phishing attacks are :

Deceptive Phishing

A criminal impersonates a recognized sender to get information like personal data or login credentials.

Sender's email should be read carefully not just the sender's name. Generic greetings, unprofessional grammar and spelling are common indicators of deceptive phishing.

Spear Phishing

Aimed at specific individuals or companies. The scammers use personalized information to lull victims into a false sense of security, convincing people to share their sensitive information. Spear phishing often contains malicious attachments or links to websites that seem legitimate.

Even if the source seems trustworthy one needs to be careful when receiving unexpected emails.

Clone Phishing

Hacker creates almost identical versions of legitimate emails from reputable sources in a clone phishing attack to trick intended victims into sharing sensitive information. A clone phishing scammer will often claim to resend an email because of an incorrect link or a missing attachment to trick the recipient into clicking them and thereby downloading malware onto the victim's device.

Before clicking a link in an email, it is advisable to hover over the link to verify the URL first.

Vishing

Vishing refers to Voice phishing or phishing over the phone. The scammers often spoof their phone numbers so they can appear to be calling from a trusted source such as a Bank. These scams typically create a sense of urgency or fear to trick a victim into giving up sensitive information.

Legitimate institutions never ask for sensitive information such as Transaction OTP, Account number, Login credentials etc.

Smishing

Smishing refers to SMS phishing or phishing via SMS text message. With smishing, criminals trick people into clicking links to malicious websites. These texts appear to be from trustworthy sources and entice victims by offering a coupon code or a chance to win a free prize.

Links in unsolicited text messages should never be clicked.

Pharming

Pharming is a sophisticated type of phishing attack where a scamster can redirect victims to the site of their choosing. They do this 'cache poisoning' by targeting the Domain Name System (DNS).

Before entering login credentials it should be ensured that the URL starts with "HTTPS".

HTTPS Phishing

In an HTTPS phishing attack the scams are hosted on malicious web addresses that include both the HTTPS designation and the padlock icon.

Ascertaining source of URL is essential for ensuring safety.

Evil Twin Phishing

An evil twin attack is when a malicious wireless access point is disguised as a trustworthy Wi-Fi network. These types of phishing attacks are often called the "Starbucks scam" because it mostly happens in coffee shops. Once someone connects to a fake wireless network, the attacker can steal account credentials the user accessed while using the network.

It is advisable to avoid accessing private accounts when connected to unsecured private wireless networks or a VPN should be used to keep data secure.



DO's & DONT's



- ✓ Stay vigilant
- ✓ Read the entire content of email not just the sender's name
- ✓ Watch out for shortened links, unprofessional language, grammar mistakes, poorly constructed statements
- ✓ Ascertain source of URL before clicking
- ✓ Check for 'https' in the URL
- ✓ Be wary of threats and urgent deadlines
- ✓ Always have upgraded Antivirus installed in your device

- Do not click on links in unsolicited text messages X
- Do not divulge sensitive information under any circumstance – Legitimate institutions never ask for them X
- Do not access accounts when connected to unsecured private networks X
- Do not respond to calls/texts promising windfall gains X