IMPORTANT LINK:

24x7 Cyber Crime Helpline

Complain any cyber crime here. Also if you need professional service.

https://www.facebook.com/24x7CyberCrimeHelpline/

Phishing:

Phishing scams are attempts by scammers to trick you into giving out any of your personal information such as your bank account numbers, passwords and credit card numbers, via Electronic communication channels, which can vary from Internet applications like, Facebook, Gmail, Yahoo Mail, Outlook/Hotmail, WhatsApp, Skype, Matrimonial Websites to even Landline or Mobile.

Phishing email messages, websites, and phone calls are designed to steal money. Cybercriminals can do this by installing malicious software on your computer or stealing personal information from your computer. Alternatively, the scammer may alert you to 'unauthorised or suspicious activity on your account'. You might be told that a large purchase has been made in a foreign country and asked if you authorised the payment. If you reply that you didn't, the scammer will ask you to confirm your credit card or bank details so the 'bank' can investigate. In some cases the scammer may already have your credit card number and ask you to confirm your identity by

Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your university, your Internet service provider, your bank). These messages usually direct you to a

spoofed website or otherwise get you to divulge private information (e.g., passphrase, credit card, or other account updates). The perpetrators then use this private information to commit identity theft.

The scammer asks you to provide or confirm your personal details. For example, the scammer may say that the bank or organisation is verifying customer records due to a technical error that wiped out customer data. Or, they may ask you to fill out a customer survey and offer a prize for participating. These scams attempt to trick recipients into responding or clicking immediately, by claiming they will lose something (e.g., email, bank account). Such a claim is always indicative of a phishing scam, as responsible companies and organizations will never take these types of actions via email or phone or via any type of online communication channels like facebook, whatsapp etc.

Phishing messages are designed to look genuine, and often copy the format used by the organisation the scammer is pretending to represent, including their branding and logo. They will take you to a fake website that looks like the real deal, but has a slightly different address. For example, if the legitimate site is 'www.realbank.com.au', the scammer may use an address like 'www.reallbank.com'.

Warning:

You receive an email, text or phone call claiming to be from a bank, telecommunications provider or other business you regularly deal with, asking you to update or verify your details.

The email or text message does not address you by your proper name, and may contain typing errors and grammatical mistakes.

The website address does not look like the address you usually use and is requesting details the legitimate site does not normally ask for.

If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown

in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address. Links might also lead you to .exe OR .vb OR .jsp OR .apk files. These kinds of file are known to spread malicious software.

Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.

Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.

Example:

ORIGINAL	PHISHING SCAM
www.facebook.com	www.faceboook.com
www.gmail.com	www.gmaiil.com
www.icicibank.com	www.icicbannk.co.in
www.onlinesbi.com	www.onlinesbibank.com
www.axisbank.com	www.axisbanks.com
www.incometaxindiaefiling.gov.in	www.incometaxindiagov.in

Prevention:

Keep all systems current with the latest security patches and updates. Use genuine Windows OS, Don’t download from Torrent.

Install an good antivirus solution, regularly check for updates, and monitor the antivirus status on all equipment.

In case of companies/corporate, Train employees to recognize phishing attacks to avoid clicking on malicious links. For example, if the domain of the link to which you are being directed doesn't match the purported company domain, then the link is a fake.

Use two factor authentication for your email accounts.

Perform a monthly security checkup of all your digital devices like, computer, laptop, mobile, tablet etc. from Professionals.

Make a habbit to follow technical and security blogs to remain updated.

IMPORTANT LINK:

24x7 Cyber Crime Helpline

Complain any cyber crime here. Also if you need professional service.

https://www.facebook.com/24x7CyberCrimeHelpline/