Leading a Secured Digital Life.....

INFORMATION SECURITY AWARENESS

www.infosecawareness.in

Information Security
Education & Awareness Team
C-DAC Hyderabad

सत्यमेव जयते

Ministry of Electronics &
Information Technology
Government of India

keeping yourself and

your family safe in a tech driven world

www.infosecawareness.in

Toll Free No: 1800 425 6235

Phishing Attack

What is Phishing Attack?

- Phishing is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity through electronic communication like e-mail , telephone call or text message.
- Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Phishing techniques

- Filter Evasion
- Phone Phishing

And so on….

Threats by phishing attacks

- Spoofing popular websites or companies.
- Scam artists use graphics in email that look identical to legitimate websites but actually it takes 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.
- Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license.

How does a phishing email message look like?

- Spelling and grammar.
- Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

How I can recognize a message of phishing?

- Normally phishing e-mails display grammatical errors or overlapped text.
- Test using false data before putting in actual information.

What should I do if I think I've responded to a phishing scam?

- Change the passwords or PINs of all your online accounts that you think could be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent e-mail.
- Routinely review your bank and credit card statements for unexplained charges or inquiries that you didn't initiate.

Guidelines for Phishing Attack

Do's:-

- Be cautious about opening any attachments or downloading files you receive from strangers.
- Look for the sender's email ID before you enter/give away any personal information.
- Use frequently updated antivirus, antispyware and firewall software.
- Always update your web browser and enable phishing filter.
- If you receive any suspicious e-mail do call the company to confirm if it is legitimate or not.
- Do use a separate email accounts for shopping online, personal etc.

Don'ts:-

- Don’t reply to any e-mail or pop-up message that asks for personal or financial information.
- Don’t open attachments that you were not expecting, especially ZIP files and NEVER run .exe files.
- Don’t use your company e-mail address for personal things.
- Don’t open any spam e-mail.
- Don’t open suspicious videos or images in social networking sites since social networking are prime target of phishing.
- Never respond to phone calls asking for bank details. It might be vishing (voice phishing). Beware of phishing phone calls.

Follow us
www.infosecawareness.in

https://www.facebook.com/infosecawareness

https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA

https://plus.google.com/u/0/106937869860139709031/posts

Email id: **isea@cdac.in**

TOLL FREE No. 1800 425 6235