NAWA Media

Phishing Attacks

Section: 4.2

What are Phishing Attacks?

Have you ever received a link randomly asking you to check out a photo or a funny filter. It is most likely that such ‘random’ links are malicious links and if they are opened they could steal your data or take control over your device.

These links are very dangerous and given the pervasiveness in these attacks, everyone should always be careful when opening up any links sent by anyone.

Basics of Strong Passwords

If you receive a link from anyone, out of the blue, check for the following things before you open the link:

- Does the link have an HTTPS protocol? If not, the website is insecure and should not be opened until you verify with the sender why they sent it. (Preferably, if its a friend, check with them using another chat platform)
- Are the spellings in the name of the website in the URL correct? Spellings and other such small details are dead giveaways of bad/ malicious links.
- If it›s a link claiming to be a Google or Facebook link, do a quick internet search to see if others are complaining of phishing attacks from similar-looking URLs and emails.
- Another dead giveaway is when an email or message asks you to change your password by clicking a link. If this email has been received without you prompting a password change, then do not open that link. However, what you must do is still change your password but go through the website and do it directly there.
- Google has developed a game that anyone can play to understand phishing better. It gives useful tips on how to avoid getting phished.

The Phishing Game

You can play it through this (VERY SAFE) and try his quiz as well:

phishingquiz.withgoogle.com

NAWA Media

We hope this course has helped in making online spaces safer for you. Feel free to share with your peers and colleagues!

BCMCR | Birmingham Centre for Media and Cultural Research

BIRMINGHAM CITY University

MEEDAN

Check

Sida