Cybersecurity Tips and Safe practices

What is PHISHING…

Phishing is a kind of Cyber-attack, making you to click on a bad link or download a malicious attachment, which are sent in Emails, social media posts or direct messages.

If you click on a phishing link or file, you will potentially hand over your sensitive personal information to the cybercriminals. A phishing scheme can also install malware onto your device.

No need to fear though! Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day.

See it so you don't click it.

Before clicking any links or downloading attachments, take a few seconds (like literally 4 seconds) and ensure the email looks legit. Once you recognize a phishing attempt you can avoid falling for it.

Here are some quick tips on how to clearly identify a phishing email:

- *Does it contain any offer which is impractical?*
- *Does it include language that's urgent, alarming, or threatening?*
- *Is it poorly written with misspellings and bad grammar?*
- *Is the greeting ambiguous or very generic?*
- *Does it include requests to send personal information?*
- *Does it stress an urgency to click on an unfamiliar hyperlinks or attachment?*
- *Is it a strange or abrupt business request?*
- *Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.*

Yes, once see a phishing email. What do I do?

Don't worry…..If you're at the office and the email came to your work email address, report it to your IT wing as quickly as possible.

If the email came to your personal email address, Do not click on any links – even the unsubscribe link – or reply back to the email. Remember, DON'T CLICK ON LINKS, JUST DELETE.

You can take your protection a step further and block the sending address from your email program."

Cybersecurity Tips and Safe practices

Why is Password Security Important?

Password security is important because passwords are the first line of defence against cybercriminals and their unauthorized access to your personal data.

Creating a strong and secure password can reduce the risk of cybercriminals guessing your password and accessing sensitive data. This is especially important for accounts containing sensitive information, such as financial email and social media accounts.

Tips On How to Create and Secure Password:

1. *Never use your name, age, birthday, phone number, address, place or any other sensitive personal information as part of your password.*
2. *Use unique password for each account.*
3. *Make long passwords by mixing upper case, lower case, Numbers and special characters.*
4. *Enable Multi-factor authentication.*
5. *Regularly change passwords.*
6. *Your web browsers' capacity to remember passwords can cause password issues. Hence, never opt for remember password facilities on personal computers.*

7. *Never write down your passwords anywhere.*
8. *Don't enter passwords where someone may be able to see you typing.*
9. *Never send passwords by email.*
10. *Don't re-use passwords after giving them a break.*

"The more complex the password, the more protected your information"

Cybersecurity Tips and Safe practices

What is Social Engineering?

Social engineering is the art of manipulating, influencing, or deceiving a person in order to gain control over his/her computer system. At its core it is manipulating a person into knowingly or unknowingly giving up information.

Phishing is one of the main deceptive techniques of social engineering. The practice of sending fraudulent communications that appear to come from a reputable source. Phishing is of three types i.e Email Phishing, Smishing and vishing.

Tips to avoid Social Engineering attacks:

1. *Avoid clicking unfamiliar links received through e-mails/messages. It may steal your personal data from your device.*
2. *Always verify authenticity of e-mail/messages.*
3. *Do not open attachments received from unknown sources.*
4. *Regularly scan your device with updated anti-virus.*
5. *Emails or messages that create a sense of urgency is a warning.*
6. *Recognize inappropriate requests for information.*
7. *Don't give any information without proper identity check.*
8. *Understand what information you are putting on social media.*
9. *Don't access confidential information at public places.*
10. *Change password regularly.*

Beware of fake messages/emails containing links/attractive offers/gifts/rewards.
Be Cyber Smart!

Cybersecurity Tips and Safe practices

What is an IoT device and how to protect IOT device?

The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. IoT devices are pieces of hardware, such as gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks.

Cyber criminals can target your unsecured IoT devices such as smart phones, smart home and Office appliances (Wi-fi Devices and Smart Printers) and can gain access to perform malicious activities.

Tips to secure IoT devices:

1. *Always Patch IoT devices (Wi-fi devices, Smart Printers) with latest software and firmware updates to mitigate vulnerabilities.*
2. *Avoid using default usernames and Passwords.*
3. *Use strong passwords and change them regularly.*
4. *Apply updates/Patches provided only by the manufacturers.*
5. *Regularly monitor IoT devices behaviour.*
6. *Remove/uninstall unwanted applications.*
7. *Regularly scan your device with updated anti-virus.*
8. *Report immediately to concerned authorities if any unauthorised activity is detected. Report to IT wing if any such activity is observed in the Office systems.*

Keep Your Internet of Things (IoT) devices secured. Be Cyber Smart!

Cybersecurity Tips and Safe practices

What is Software vulnerability and Patch? How to ensure cyber security?

A security flaw, glitch, or weakness found in software code that could be exploited by an attacker is called as Software vulnerability. Whereas, Patches are software and operating system (OS) updates that address vulnerabilities within a program or product.

The software developers do their best to safeguard our cyber security by coming up with the latest versions which includes patches to the known vulnerabilities in the existing system, all we need to do is update them at our end. By promptly installing these necessary updates duly taking into consideration the application dependencies, we can ensure that our systems remain secure against any emerging threats

Tips to secure system against vulnerabilities:

1. *An essential step in preventing and identifying infections based on vulnerability in the system is installing antivirus software solution.*
2. *Turn on Automatic Updates. This is the simplest way to ensure that your computers and other devices are constantly up-to-date.*
3. *Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.*
4. *Make sure to keep all the applications in the system are up-to-date.*
5. *Ensure you're staying cyber secure by ensuring your operating system is always up-to-date.*

Don't wait, update your device before it's too late.