ONLINE SECURITY AND PRIVACY

The open and global nature of the Internet has made life easier and less private. Internet security is important to protect our privacy, protect us from fraud and identity theft. Internet security protects personal information from attacks, theft and misuse, thereby ensuring privacy safeguard.

Internet users need to improve their information security and privacy. People, without realizing provide personal information on the Internet which can be misused by cybercriminals for identity theft. Information on the Internet cannot remain safe and private if there are no security measures in place.

ONLINE ATTACKS

1. Social Engineering

Social engineering is a non-technical method of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that people encounter today.

A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural thoughtfulness of people, as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

A Common form of Social Engineering attack is Email from a friend. If a criminal manages to hack or socially engineer a person’s email password they have access to that person’s contact list, and because most people use one password everywhere, they probably have access to that person’s social networking contacts as well.

Once the criminal has that email account under their control, they send emails to all the person’s contacts or leave messages on all their friend’s social pages, and possibly on the pages of the person’s friend’s friends. These messages may:

- **Contain a link** that you just have to check out, and because the link comes from a friend and you're curious, you'll trust the link and click – and be infected with malware so the criminal can take over your machine and collect your contacts' information and deceive them just like you were deceived.

- **Contain a download** – pictures, music, movie, document, etc., that has malicious software embedded. If you download, which you are likely to do since you think it is from your friend, you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know.

2. Phishing

Phishing is essentially an online con game and phishers are nothing more than tech-savvy con artists and identity thieves. They use spam, malicious web sites, email messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts.

How to know you're being "phished":

- Phishers, pretending to be legitimate companies, may use email to request personal information and direct recipients to respond through malicious web sites;

- Phishers tend to use emotional language using scare tactics or urgent requests to entice recipients to respond;

- The phish sites can look remarkably like legitimate sites because they tend to use the copyrighted images from legitimate sites;

- Requests for confidential information via email or instant messages tend not to be legitimate;

- Fraudulent messages are often not personalized and may share similar properties like details in the header and footer.

3. Malware

Malware is a category of malicious code that includes viruses, worms, and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms

sent through email and instant messages, Trojan horses dropped from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy.

Malware works to remain unnoticed, either by actively hiding, or by simply making its presence unknown on a system which is known to the user. Hence, only antivirus or antispyware can recognize its presence.

4. Pretexting

Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

5. Quid Pro Quo

A quid pro quo is when an attacker requests personal information from a party in exchange for something desirable. For example, an attacker could request login credentials in exchange for a free gift.

6. Spear Phishing

Spear phishing is like phishing, but tailored for a specific individual or organization. In these cases, the attacker is likely trying to uncover confidential information specific to the receiving organization in order to obtain financial data or trade secrets.

7. Tailgating

Tailgating is when an unauthorized party follows an authorized party into an otherwise secure location, usually to steal valuable property or confidential information. This often involves subverting keycard access to a secure building or area by quickly following behind an authorized user and catching the door or other access mechanism before it closes.

TIPS ON HOW TO STAY SAFE:

1. Mobile/Smart Phones

Mobile phones can be categorized as all phones that have the capacity of voice and simple text messaging services. But advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers which are tagged as smartphones. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a Wi-Fi connection (similar to a laptop at an internet café) or via data connections through the mobile network operator.

Smartphones now usually support wide range of functionalities i.e. web browsing, e-mail, voice and instant messaging, mobile banking etc. over the internet.

However, many of these tools and features introduce new security issues, or increase existing risks. Some important ways to secure your smartphones:

- Keep your phone with you all the times. Never leave it unattended. Avoid displaying your phone in public.
- Most commonly used smartphones are Apple's iPhone, Google's Android, followed by Blackberry and Windows phones; it is important that a user ascertains what services a smartphone best offers to suit him/her. For example, Blackberry phones have been presented as secure messaging and e-mail devices.
- It is recommended that you buy an unlocked smartphone. A locked phone poses a higher risk since all your data is routed through one carrier. If your phone is locked, ask someone you trust about unlocking it.
- Install new software on your smartphone via corresponding trademarked software store e.g. Apple's iPhone uses iPhone Appstore, Google's Android uses Google Play-store. Create account and log-in with your credentials to download and install the desired application.
- When disposing of your phone, make sure you are not giving away any information that is stored on the phone, the SIM or memory card (even if the phone or cards are broken or expired).
- Refrain from connecting personal devices to free Wi-Fi networks, as you would give hackers total access to that device - there's nothing like a "*free lunch*".

2. Personal Computers/Laptops

It is a known fact that man's best friend is now the device(s) he/she owns, which contains so much information that once in the wrong hands, can prove harmful. Access to device(s) is the easiest way for hackers to steal personal/private information. A few points to note:

- Ensure you set a strong password to unlock your device(s), and change it as often as possible.
- Create a user account with restricted access, and log into your system with that profile. Only make use of the administrative profile when that level of authentication is required e.g. installation.
- When permitting others to make use of your personal system, ensure a profile with restricted access is used.
- Disable the guest user account.
- It is good practice to always backup data from your device as often as possible.
- Always update Windows and web browsers.
- Ensure the antivirus is always up-to-date, and run daily/weekly scans.
- Make use of encryption where available.

3. External Devices

It is almost impossible to abstain from the use of external devices on computer systems; as such it is necessary to be a bit more cautious. Some points to note:

- Once an external drive is inserted to your system, check that the antivirus scans the drive immediately, which should be automatic. If it isn't, have the automatic feature enabled, otherwise perform a manual scan of the drive.
- Refrain from using USB drives containing private/confidential documents on public computer systems/networks or cyber cafes.
- Do not save confidential files on public or unsecured network file servers.

4. Internet Safety

It is essential to always take extra measures while on the Internet:

- If uncertain about the source of a hyperlink, hover over the link without clicking it. You will notice the full URL of the link's destination usually in the lower left corner of your browser window.

- When online, avoid clicking on hyperlinks to ensure you do not download any malware that may be masked by the link; always copy and paste the link into the address bar of your browser – right-click the link to bring up the context menu, then click Copy shortcut (in Internet Explorer), Copy Link Location (in Firefox), or Copy Link Address (in Chrome).
- Always ensure your browser is up-to-date.
- Once online transactions are concluded and you have logged off, always close the browser to ensure the session becomes "inactive".
- If your online session terminates inappropriately, ensure you log back in and log off properly.

5. Email/Instant Messaging

- Only open email or instant messaging (IM) attachments that come from a trusted source;
- Have email attachments scanned by renowned anti-virus prior to opening;
- Delete all unwanted messages without opening;
- Do not click on web links sent by someone you do not know;
- If a person on your buddy list is sending strange messages, files, or web site links, terminate your IM session;
- Scan all files with an Internet security solution before transferring them to your system;
- Only transfer files from a well-known source;
- Use renowned anti-virus to block all unsolicited outbound communication;
- Keep security patches up to date;
- Report to the relevant security agents if you believe you are a victim of cyber-attack in any form, or report via the consumer web portal and it will be re-directed to relevant department/agency.