ISSUE NO 02

SEPTEMBER 2023

Cyber Guardian

Publication for your online safety

Warning

Mobile phones

are the latest target of hackers

Recent reports reveal that portable devices like mobile phones, and tabs have become the latest targets of cybercriminals.

According to these reports, the proliferation of mobile phones, and the fact that they often contain personal data, passwords, and corporate information, made it easy approach for cybercriminals to steal passwords and then gain access to company networks.

Many company employees use their mobile devices to access their company networks. It is as high as 39%, according to the Finance Online Statistics report. Hacking this device easily allows cybercriminals to gain access to company data.

The amount of data contained in mobile devices is so high that if hacked, it allows users to gain access to sensitive information including credit card details, social media accounts, and even 'eavesdrop' on confidential conversations by taking control of its camera and microphone.

A significantly higher percentage of mobile device users spend time accessing the Internet via unsecured networks and unsecured locations outside the corporate network (e.g.: FreeWiFi), making them easy targets for hackers. Forbes puts this percentage at 80%. And nearly 70% of online fraud is done through mobile platforms, they say.

Many organizations opt for a bring-your-own-device (BOYD) policy for company work, making it easier for hackers to access the device and thus the company network.

Security

Beware of ransomware extortionists

Ransomware is malicious software that holds an individual or organization's data hostage until a ransom is paid.

In this cybercrime, access to information on computer networks, mobile devices and server computers is blocked and victims are pressured to make a payment to release the data.
Payment is usually requested via Bitcoin. That is cryptocurrencies whose owner is difficult to trace.

How can you protect your devices from ransomware infection?

Avoid clicking on links in spam email messages or on unknown websites. If you click on malicious links, an automatic download may be initiated and your computer may be infected.

Avoid revealing personal information: If you receive a call, text or email from an untrustworthy source asking for personal information, do not answer. Do not open suspicious email attachments Avoid opening any suspicious-looking attachments.

Do not connect USB or other storage media that you obtained in an untrusted manner to your computer. Only open the attachments that are trustworthy and rely only on verified and trusted websites for downloads.

Backup all important information. Check that they are working regularly. Keep your operating system and software up to date with the latest patches. Maintain up-to-date anti-virus software, and scan all software downloaded from the Internet before running.

Avoid enabling macros from email attachments. Educate and encourage employees to participate in cyber security awareness training.

Hot Line -101 report@cert.gov.lk www.cert.gov.lk www.onlinesafety.lk

Confidential

PASSWORD

IS PRIVATE AND CONFIDENTIAL

This Cyber Security Month, many countries are focusing on some basic behaviors that every citizen of the society should follow for cyber security as members of the digital society. The use of a strong password is key. Change passwords from time to time.

Do not use the same password for several online platforms or accounts. A password should consist of at least ten characters, including uppercase letters, lowercase letters, digits, and special characters for strength. It is important to enable two-factor authentication.

Also, updating your software from time to time and enabling automatic updates, equipping yourself with Firewalls and Network Security, using only secure websites, using HTTPS for secure Web Browsing, avoid opening suspicious file attachments and avoid clicking on unknown and suspicious links when using emails, keeping regular backups etc. is vital.

Risk

Social media - your character certificate

It will be important to pay attention to a few things that need to be taken care of when using social media such as Facebook, which is very popular today. It is important to decide who can see your profile information such as email address, phone number, photos, etc. It is important that it is set for friends only.

Be especially careful with photos or other content that you don't want to share publicly. Society will determine what kind of person you are by the information you share on social media. It is your own character certificate.

Since your information statements are a mirror that shows your image, consider that they may be used against you in the future. When looking for a new job, you should think that this is the first place a prospective employer will find information about you. Careful awareness of these areas will determine the ability of the country's digital development to proceed more safely.

Beware

Cyber Violence against Women and Girls

Particularly, as a woman when you go online, there are hurdles that bring safety issues that a man does not usually experience. Cyber-bullying, sexual harassment, doxing, threatening, and disclosing private photos and videos without consent are some issues faced by women in cyberspace. These are gender-based abuses in cyberspace.

You as a smart woman, should always take the responsibility to stay aware of the dangers that exist in cyberspace, and should develop your skills to protect yourself from gender-based cyber abuses.

Following are some common online threats as a woman you might get exposed to,

Cyber-bullying

Cyberbullying is the usage of social media, emails or mobiles to embarrass, degrade, threaten or silence an individual. You may encounter the following issues on Facebook, WhatsApp, Viber, Instagram, and other social media platforms.

Sexting

Sexting is circulating sexually explicit messages, photographic images or videos through social media platforms. Someone can circulate sexually explicit images of you to others or even can post such photos on a social media platform.

Doxing

Doxing is someone distributing your personal information such as your home address, phone number, email address or place of work without your consent. Such information can be used by the perpetrator to blackmail you or impersonate you.

Cyberstalking

Cyberstalking is someone gathering your personal data available online (your financial affairs, relationship details, social and work life, your location) to stalk you or harass you, or even to establish a relationship with you.

Revenge porn

Revenge porn means distributing sexually explicit photos or videos of yourself onto social media or uploading such content to pornographic websites. Typically, the content of this nature can be posted by your ex-partner (boyfriend), who does it with the purpose of causing humiliation and damage to your reputation.

If you face such threats, you can block those individuals, complain to the relevant social media platform, and even seek the legal assistance for further actions.