GUIDELINES FOR PARENTS AND EDUCATORS

SECURE PASSWORDS

The Importance of Strong Secure Passwords
A strong password serves as your primary defense against unauthorized access. Passwords function like the keys to your online accounts and personal information.

What Constitutes a Strong Secure Password?
Security experts recommend using a "passphrase" instead of a simple, traditional password. This phrase should be relatively long—8-12 characters or more - and consist of seemingly random words combined with numbers, symbols, and both upper and lower case letters. It should be something personally memorable but difficult for others to guess. Personal information and/or common words should be avoided.
Symbols, such as using "$" in place of the letter "S," or including symbols like "&" or "%" should be incorporated. However, it should be cautious; $1ngle is NOT a good password, as password thieves are aware of such combinations. In contrast, Mbf$TJ1ravng (short for "My best friend Sam T Jones is a very nice guy") is an excellent example of a strong password.

Should the Secure Password Be Changed and How Frequently?
It is wise to change the security password periodically, just like cleaning the house! This practice is known as cyber hygiene and is crucial for online security.

Is It Recommended to Share Secure Passwords with Others?
As a general rule, personal security password should be never shared with anyone. However, there may be instances where sharing could be beneficial, such sharing children's security passwords with you as parents. Even with friends, kids shouldn't share passwords. Explain that sharing passwords is like giving away their house keys.
Even more, while it may seem obvious, studies reveal that the security passwords are usually shared on sticky notes attached to computer monitors. This is a bad idea. If you must write it down, ensure the note is properly hidden.

Is It Safe to Use the Same Password Across Multiple Sites and Apps?
No, it is not safe. If any of your accounts are hacked or if someone associated with that site steals your password, criminals may attempt to use it on other sites and applications. It's best to differentiate your passwords by adding unique letters, numbers, or symbols for each account.

Understanding Multi Factor Authentication?

Often referred to as two-factor authentication (2FA), multi-factor authentication adds an additional – usually optional – "step" to access an account, device, or document.

Numerous services, including banking and social media platforms, provide multi-factor authentication as an option to enhance the security of your accounts beyond just a strong password. Typically, this involves receiving a text or another type of message on a registered mobile device containing a code that you must enter to confirm your identity. Additionally, there are apps available that can generate these codes. In most instances, you won't need to use this code when logging in from a recognized device, such as your computer, tablet, or phone. Keep in mind that incorporating a second step for logging in (like a code sent to your phone) significantly boosts your security!

It is highly recommended to use a strong password, along with multi-factor authentication, whenever possible.

More Ways to Stay Safe

Utilize a Password Manager
Help your family stay safe by using a password manager like RoboForm or LastPass. These programs and web services work on personal computers and mobile devices, and they create strong, unique passwords for each of your accounts — so you don't have to remember them all. Browsers like Chrome, Safari, and Edge also have free built-in password managers. You'll just need to remember one strong "master" password to access the program or secure site that stores all you passwords. Make that master password very strong — if someone gets it, they could access all your accounts.

Beware of Phishing Attacks
Exercise caution before clicking any link — even if it appears like it's from a trusted source. If a message asks you to log in, change your password, or give personal information, it might be a phishing scam trying to steal your data - remember it could be legitimate or part of a phishing scam designed to capture your data for malicious purposes. It is recommended to type the website address (URL) directly into your browser instead of clicking links.

Ensure Devices Protected
Malicious software - viruses and spyware, like keyboard loggers (which can track your typing), can be used to steal your security passwords. Protect your devices by using up-to-date antivirus or anti-malware software. Also make sure your operating system, applications, and browser are fully updated.

Use Fingerprint or Face Unlock on Your Mobile Devices
Most smartphones can be secured with a code, typically a number sequence or a pattern drawn on the screen. Many also allow you to register your fingerprints, providing a high level of security (Rest assured, your fingerprint or facial data remains on your device and is not shared with any other.)

Check and Talk About Accounts Regularly
Regularly review your child's online accounts together. Help in updating security passwords and teach them how to recognize anything suspicious — like strange messages or login alerts.

For detailed info, visit our website www.mksafenet.mk

Be careful before clicking on a link (even if it appears to be from a legitimate site) they will never ask you to change your password or give personal information.

Co-funded by the European Union