

3. Protect your passwords

CYBERSECURITY

SUMMER

3

PROTECT YOUR PASSWORDS.



Create Strong Passwords	Use Unique Passwords for Different Accounts	Our cybersecurity, Everyone's accountability for more INFO and TIPS  Questions? ict@intersoft-electronics.com
Change Passwords Regularly	Use a Password Manager	
Enable Multi-Factor Authentication (MFA)	Secure Your Devices	
Avoid Password Sharing	Monitor for Data Breaches	
Log Out from Shared Devices	IE  CYBER SECURE	

In summary, Password protection is a fundamental aspect of digital security. By creating strong, unique passwords and implementing additional security measures such as MFA and password managers, you can significantly reduce the risk of unauthorized access to your accounts. Staying vigilant and proactive about password security will help protect your personal and professional data from cyber threats.

Password protection is essential for safeguarding your personal and professional information from unauthorized access. Strong passwords are a critical defense against cyber threats such as hacking, identity theft, and data breaches. Here's why password protection is important and how you can enhance your password security:

1. WHY IS THAT SO IMPORTANT?

1. Prevent Unauthorized Access
 - Strong passwords ensure that only authorized individuals can access your accounts and sensitive information.
2. Protect Personal Information
 - Your personal information, such as financial data, project records, and personal communications, remains private.
3. Secure Financial Assets
 - Passwords protect online banking, shopping, and other financial services from fraud and theft.
4. Safeguard Professional Data
 - In a work environment, passwords protect confidential company information, proprietary data, customer data and internal communications. Remind that a lot of data in our company is bound to NDA's and confidential agreements. If you are in doubt about the level of confidentiality of data, ask your department lead or deal with it as being confidential.
5. Mitigate Cyber Threats
 - Strong, unique passwords reduce the risk of being compromised by malware, phishing, and brute-force attacks.

2. HOW TO PROTECT YOUR PASSWORDS EFFECTIVELY

1. Create Strong Passwords
 - Length and Complexity: Use a combination of at least 12 characters, including uppercase and lowercase letters, numbers, and special symbols.
 - Avoid Common Words: Don't use easily guessable words, names, or dates such as "password", "123456", or your birthdate.
 - Passphrases: Consider using a passphrase – a sequence of words or a sentence that is easy for you to remember but hard for others to guess (e.g., "Myp@ssw0rd!isStr0ng").
2. Use Unique Passwords for Different Accounts
 - Never reuse passwords across multiple sites. If one site is compromised, reused passwords can allow access to other accounts.
3. Enable Multi-Factor Authentication (MFA)
 - MFA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone or a biometric factor like a fingerprint.
4. Change Passwords Regularly
 - Update your passwords periodically, especially for accounts that contain sensitive information.
5. Use a Password Manager

- Password managers securely store and generate complex passwords for you, so you only need to remember one master password. KeePass is installed on every PC delivered by IT.
6. Monitor for Data Breaches
 - Use services like Have I Been Pwned to check if your email or passwords have been involved in a data breach. Change your passwords immediately if a breach is detected.
 7. Avoid Password Sharing
 - Never share your passwords with others. If you must share access, use features like delegation or role-based access instead of sharing your credentials.
 8. Secure Your Devices
 - Ensure your devices are protected with passwords, PINs, or biometrics. Keep your operating systems and software up-to-date to protect against vulnerabilities.
 9. Log Out from Shared Devices
 - Always log out of your accounts when using shared or public computers to prevent unauthorized access.

3. IN SUMMARY

Password protection is a fundamental aspect of digital security. By creating strong, unique passwords and implementing additional security measures such as MFA and password managers, you can significantly reduce the risk of unauthorized access to your accounts. Staying vigilant and proactive about password security will help protect your personal and professional data from cyber threats.

4. ADDITIONAL TIPS

- **Educate Yourself and Others:** Stay informed about the latest cybersecurity threats and best practices. Educate your colleagues on the importance of password security.
- **Regular Backups:** Regularly back up your important data to protect against data loss from hacks or malware attacks.
- **Use Encrypted Connections:** When accessing accounts online, ensure you use secure connections (HTTPS) and avoid using unsecured public Wi-Fi networks without a VPN.



Together we keep InterSoft Electronics cyber secure

INTERSOFT ELECTRONICS NV
Lammerdries-Oost 27 | B-2250 Olen | Belgium
Tel +32 14 23 18 11 | support@intersoft-electronics.com