

Cybersecurity Home Checklist

Cybersecurity best practices help protect your family against common threats such as data breaches, password-based attacks and social engineering. Follow these basic steps to Flex Your Cyber at home!

EVERY DAY

- ☐ **Use strong and unique passwords**
At least 16 characters with uppercase and lowercase letters, numbers and symbols. Alternatively, use passkeys when available. A secure password manager can create and store passwords and passkeys for you.
- ☐ **Enable MFA for every account**
Multi-Factor Authentication (MFA), also known as 2FA, adds an extra layer of security, such as a one-time code or biometrics, for accessing your online accounts.
- ☐ **Avoid oversharing on social media**
Keep your social media accounts private and accept friend requests only from people you know. Don't share your location, birthday or unnecessary personal information.
- ☐ **Learn to recognize phishing attacks**
Watch for unexpected requests for sensitive information and inconsistencies in email addresses and URLs. Don't click suspicious links or attachments.
- ☐ **Browse safely**
Only use secure WiFi networks and avoid public WiFi. Secure your home network with a strong password and enable network encryption.
- ☐ **Use antivirus software**
Antivirus software helps prevent, detect and remove known viruses and malware before they can infect your devices.
- ☐ **Secure your devices**
Log off when leaving your computer unattended. Always use a screen lock, such as a code or biometrics, to protect your mobile devices.
- ☐ **Start a dialogue**
Stay up to date on the latest cybersecurity threats and best practices, and discuss cyber safety and security with your family using age-appropriate language. Encourage children to tell you about anything concerning or suspicious.

EVERY MONTH

- ☐ **Back up your data**
Ensure you have a safe copy of important files, photos and documents by backing them up to a secure cloud service or external hard drive.
- ☐ **Install new updates**
When new updates for software, devices, routers or apps become available, download them immediately, and enable automatic updates wherever possible.
- ☐ **Conduct a dark web scan**
Check if your credentials have been compromised using a free service like BreachWatch. Update any exposed passwords to ones that are strong and unique.
- ☐ **Check browser settings**
Set your family's browser security settings to the highest level that still allows effective web browsing. Check for updates, and clear your browser's cache regularly.

EVERY YEAR

- ☐ **Update parental controls and privacy settings**
Check and adjust the parental controls and privacy settings for your children's apps, gaming platforms and accounts.
- ☐ **Delete old accounts and apps**
Delete old online accounts to minimize your digital footprint and reduce the chance of old accounts being hacked. Get rid of unused apps to help maintain device performance and security.
- ☐ **Review unnecessary permissions**
In your security settings, review app permissions on your family's devices. Remove unnecessary permissions, such as access to location, contacts or other sensitive information.
- ☐ **Perform a network security audit**
Review your home network security, including router settings and connected devices. Ensure your WiFi's default name is changed, that it has a strong and unique password, and that the router's firmware is up to date.