I often click ‘remind me later’ when I get software update notifications. What’s the risk of putting off software and operating system updates?

Did you know that updates include security improvements to fix bugs on your computers and mobiles and even apps? Installing software updates will give you the latest security. You can even set them to happen automatically.

I use my pet’s name as my password, why isn’t this secure?

Do any of your social feeds mention your dog’s name? Chances are that your dog’s name is common knowledge. Cybercriminals collect information you reveal about yourself online and use this to try and crack your passwords or answers to security questions. It’s best not to use common passwords like your family members’ names, date of birth or any other easy-to-guess personal details. A strong password is a 13 character passphrase. For added security, turn on a second layer of security with two-factor authentication whenever possible.

My Wi-Fi router/modem and devices came with default (factory set) passwords, why do I need to change them?

Most new devices, like Wi-Fi modem/routers, come with a default, or factory set password. These default passwords are usually available in manufacturers’ websites or in blogs. So if you don’t change the password, they’re only a Google search away for cybercriminals!

How can I protect my kids when they’re browsing and downloading online?

Malicious software and viruses can easily download on your device if you click on untrustworthy links or visit fake websites. Protect your family by installing and automating anti-virus and browser software updates, so you’re always running on the latest versions. Talk to your children about not clicking on suspicious websites or links. And make sure your kids are only downloading mobile apps from an official app store. Advice on parental controls and other online safety tools can be found at https://www.esafety.gov.au/parents/skills-advice/taming-technology
How can I protect my family’s privacy online?

Always read sites’ policies on how your information will be used. If you’re not comfortable with the type of information being asked of you, consider if you really want to sign up. You should also review privacy and security settings to decide what personal information you want to share. Generally, the less personal information you and your family share online, the better. Encourage your kids to use a different name and pic to their own when they sign up for online social media or gaming accounts. Teach kids about what they’re potentially giving away online. And lastly, think twice about what you share about your family members – always consider who else is seeing this information.

How can I know and control what my children are doing online?

Parental controls are software tools that allow you to monitor and limit what your child sees and does online. As your child grows older however, it’s best to equip them with the skills and knowledge to protect themselves online, like warning signs for inappropriate content or malicious websites.

Why should I back up my family’s computers and devices?

To avoid losing your precious family photos, videos, personal and financial information and even your kids’ school assignments! Data loss can happen from computer malfunctions, accidental deletion and ransomware attacks. If you’ve got a recent backup (either stored on the cloud or an external drive that you disconnect from your computer), you can easily restore your data. You can setup automatic back-ups for added peace of mind.

How do I protect my family when connecting online outside of the home?

You can use your settings to disable location-sharing on mobile devices. Be careful when sharing your location online or geosharing. While location sharing may appeal to many users, it allows social media followers (or anyone, if profiles are public) to see exactly where they are. This can present physical and online risks. Similarly, it’s best to turn off Bluetooth on your device when you’re not using it. Also be family smart about using public Wi-Fi. Avoid sending or receiving sensitive information when connected to public Wi-Fi hotspots – the information being sent between your device and the public Wi-Fi network can be easily intercepted by cybercriminals.

Where do I go for help if my family or I have been a victim of an online scam or cybercrime?

If you think you’ve been the victim of an online nasty, act quickly. More advice is at https://www.staysmartonline.gov.au/get-help

MORE INFORMATION

Visit https://www.staysmartonline.gov.au
Subscribe to our Alert Service for free information on the latest online threats and scams https://www.staysmartonline.gov.au/alert-service
Follow us on Facebook https://www.facebook.com/staysmartonline