

Checklist for fixing the family devices



Cybersecurity on the Go (VPN)

- ✓ Install a VPN solution on as many devices as possible
- ✓ Choose a preferred server in a geographic location that complies with your local data processing rights
- ✓ Read the EULA to understand what is being logged, data retention policy and what the vendor may collect about you



Smart home security assessment

- ✓ Change administrator passwords for all smart devices in the household
- ✓ Build a guest network for all IoTs to 'live' on separately
- ✓ Disable features you don't need
- ✓ Monitor devices for unusual behavior (this can be automated with a router with built-in security)
- ✓ Keep IoTs up to date, make sure the latest patches are applied
- ✓ Consider a router with a built-in security hub



Password Advice and Best Practices

- ✓ Use strong alphanumeric passwords with a sprinkle of special characters (%\$^#& etc)
- ✓ Use separate passwords for different accounts to avoid compromising all your accounts in case of a data breach
- ✓ Enable two-factor authentication (2FA) on every platform that offers it
- ✓ Consider using a password manager to limit password hassle, to secure your credit card information, and to autofill online forms



Fixing the family browser

- ✓ Keep the family browser updated to ensure the latest security fixes are applied
- ✓ Fine-tune the acceptance of cookies and use 'do not track' to reduce ad targeting
- ✓ Manage site settings and permissions like location tracking, camera and microphone access, notifications and background sync
- ✓ Use 'security checkup' regularly



Fixing the Family Computer

- ✓ Make sure you have the latest updates
- ✓ Configure the system to install future updates automatically
- ✓ Tweak User Account Control Settings and Privacy Settings
- ✓ Ensure the web browser is up to date, limit browser extension use and review existing plugins and extensions
- ✓ Encrypt the computer hard drive, in case of loss or theft
- ✓ Install protection to defend against threats both known and new



Fixing and Hardening the Family Router

- ✓ Keep the router always updated
- ✓ Change default credentials and use WPA3 encryption if available
- ✓ Disable WSP and UPnP if they are not absolutely necessary
- ✓ Set up a guest network for guest devices
- ✓ Disable the web-based administrative interface
- ✓ Use a VPN tunnel if supported by your router to protect the entire household traffic
- ✓ If the device is old and needs replacing, choose a new one with built-in IoT and endpoint protection



Fixing the family printer

- ✓ Restrict cloud printing if not used
- ✓ Disable UPnP on your home network
- ✓ Set a unique password for your printer
- ✓ Make sure the printer is up to date with the latest patches applied
- ✓ Use a secured router or make sure that your Wi-Fi network requires a password



Fixing the Family Phones and Tablets

- ✓ Install protection to defend phones and tablets against malware, phishing and fraudulent links
- ✓ Install a VPN solution to get enforced encryption on the go. If possible set it to “always on”
- ✓ Check if your device is running the latest available version of the operating system
- ✓ Plan for change if your phone model is not supported anymore

