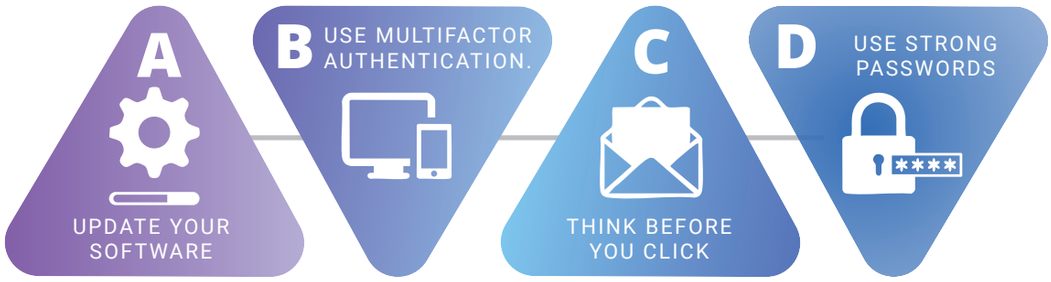
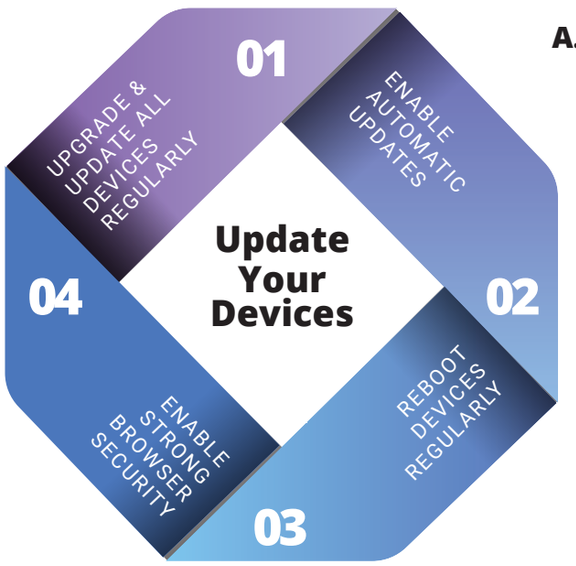
SECURITY BASECAMP

Home & Remote Work
SECURITY TIPS

A, B, C'S OF **CYBER SECURITY**





A. Update Your Devices / Operating System / Software: Keep Things Up to Date

- **Upgrade and update all devices regularly:** Ensure all equipment (routers, computers, phones, IoT devices) is running the latest software and firmware.
- **Enable automatic updates:** Activate automatic updates for your devices, especially for operating systems and routers.
- **Reboot devices regularly:** Schedule weekly reboots to reduce the chance of non-persistent malware remaining on your devices.
- **Enable strong browser security:** Use a modern browser that supports transport layer security (TLS) and keep it updated.

B. Use Strong / Unique Passwords + MFA

Use Secure Passwords

- Enable MFA on all critical accounts and services to add an extra layer of security.

Use multi-factor authentication (MFA)

- Enable MFA on all critical accounts and services to add an extra layer of security.

Remote Work Use VPN / Avoid public Wi-Fi Without VPN

- If necessary, use a VPN when accessing the internet from public hotspots.

Utilize encryption

- Enable full disk encryption on laptops, tablets, and smartphones
- Password-protect your devices (phone, iPad, laptop).

C. Be Wary of Phishing Emails

- Think before you click on a malicious link, never enter your username / password as a result of an email request).

D. Turn Firewall On Your Devices and Utilize Security Software

- Ensure your devices / router has firewall capabilities and use a security suite that includes antivirus, anti-phishing, and malware protection. Apple devices ship with protections in place, but it doesn't hurt to run a malware scan / complement with Malwarebytes.