Action for Children

Cybersecurity Tips for Remote Workers

FIRST THINGS FIRST

Take your passwords very seriously. You ARE NOT more clever than professional hackers. Use password management tools.

PASSWORD MANAGEMENT

https://www.pcmag.com/picks/the-best-password-managers

CYBERSECURITY FOR REMOTE WORKERS[1]

As more employees work from home, basic security measures need to be taken to protect the individual and enterprise from cyber criminals who are taking advantage of lax telework security practices.

THINK BEFORE YOU CLICK.

Cyber criminals are taking advantage of people seeking information on COVID-19. They are distributing malware campaigns that impersonate organizations like WHO, CDC, and other reputable sources by asking you to click on links or download outbreak maps. Slow down. Don't click. Go directly to a reputable website to access the content.

LOCK DOWN YOUR LOGIN.

Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

CONNECT TO A SECURE NETWORK AND USE A COMPANY-ISSUED VIRTUAL PRIVATE NETWORK (VPN)

---

[1] https://staysafeonline.org/wp-content/uploads/2020/03/NCSA-Remote-Working-Tipsheet.pdf

to access any work accounts. Home routers should be updated to the most current software and secured with a lengthy, unique passphrase. Employees should not be connecting to public WiFi to access work accounts unless using a VPN.

SEPARATE YOUR NETWORK

so your company devices are on their own WiFi network, and your personal devices are on their own.

KEEP DEVICES WITH YOU AT ALL TIMES OR STORED IN A SECURE LOCATION

when not in use. Set auto log-out if you walk away from your computer and forget to log out.

LIMIT ACCESS TO THE DEVICE YOU USE FOR WORK.

Only the approved user should use the device (family and friends should not use a work-issued device).

USE COMPANY-APPROVED/VETTED DEVICES AND APPLICATIONS

to collaborate and complete your tasks. Don't substitute your preferred tools with ones that have been vetted by the company's security team.

UPDATE YOUR SOFTWARE.

Before connecting to your corporate network, be sure that all internet-connected devices - including PCs, smartphones and tablets - are running the most current versions of software. Updates include important changes that improve the performance and security of your devices.