5 Tips for Remote Work Cybersecurity

Working from home is convenient for your staffers - and for cybercriminals perpetrating new attacks. Use these 5 tips to protect your systems and data from their traps.

01

Beware of videoconferencing data dangers

Make sure information like a password on a sticky note isn't visible and virtual meeting rooms are locked or encrypted to keep data safer.

02

Use multifactor authentication

80% of data breaches are caused by stolen or cracked passwords. Require a stronger credential than just a password to access systems and data.

03

Don't get hooked by phishing

Phishing is up 667% as cybercriminals spoof official-looking documents and sites. Upgrade every staffer's phishing resistance training.

04

Update every device

Failing to patch or update VPNs, devices, and software means that security might not be up to date. Update everything, every time.

05

Implement BYOD security and policies

Workers using personal devices and transferring files unsafely to them add surprise vulnerabilities. Create and enforce BYOD policies.

Sources:

UC Today - https://www.uctoday.com/collaboration/video-conferencing/video-conferencing-security-four-key-considerations/
ID Agent - https://www.idagent.com/passly
The Next Web - https://thenextweb.com/syndication/2020/04/07/why-the-coronavirus-lockdown-makes-you-more-vulnerable-to-phishing-scams/
CISA - https://www.us-cert.gov/ncas/alerts/aa20-073a
NIST-CSRC - https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

ID AGENT
A Kaseya COMPANY

www.idagent.com | sales@idagent.com