planetmagpie

I.T. SECURITY PRACTICES OF THE PROS

How do you rate?

PASSWORD POWER

□ We require employees to change their network passwords every 6 months at a minimum. Every employee must use a complex password.

□ We enable MFA (multi-factor authentication) on our cloud and office applications, whenever possible.

□ Our employees must use password vault programs (instead of browsers) to store their passwords.

NETWORK SAFETY

□ We run firmware updates on our network gear (switches, firewalls, routers, Wi-Fi) quarterly, or sooner if the manufacturer announces a security risk.

□ We conduct mitigation on exploits found in our quarterly network vulnerability testing.

□ All remote employees must use a VPN or secured Wi-Fi hotspot when accessing the company servers.

□ Our company policy on remote access forbids use of an insecure Wi-Fi connection to access the company's network.

SOFTWARE SAFETY

□ We do not run unsupported software on our servers or workstations.

□ We do not use pirated software.

□ We do not grant administrative rights to employee workstations.

DEVICE SAFETY

□ We regularly apply all security patches and Windows updates to our company workstations.

□ We implement encryption on all workstations.

□ All company workstations, devices, and mobile phones have password or PIN protection.

□ We have a corporate policy on device safety, and train our employees on how to travel safely with their company devices.

□ We asset tag our IT hardware (which forces recording of a device's details), helping police recover stolen items and assisting with insurance claims.

TEAM SAFEGUARDS

□ Our employees are not allowed to use personal email for work purposes.

□ Employees with BYOD (Bring Your Own Device) must use a segregated guest network. These devices are not allowed on the company's network.

□ We provide cybersecurity best-practice training for our employees once a year.

LEAST PERMISSION

□ We provide our employees access only to the applications required to do their job.

□ Employees cannot share accounts for workstations, online services, Office 365/Google Workspace accounts, etc.

□ We terminate all separated employees' account access immediately upon their leaving the company (including Remote Desktop Services).

BUSINESS SAFETY NET

□ We conduct monthly security patching and software updates to our servers.

□ We test our server cloud backups for recoverability at least quarterly.

□ We test our workstation cloud backups for recoverability at least quarterly.

□ We test our Office 365/Google Workspace third-party backups for recoverability at least quarterly.

□ We have a Cyber Insurance policy that protects us from loss due to cyberattack.

/ 26	0-5 Points	6-10 Points	11-15 Points	16-20 Points	21-26 Points
TOTAL SCORE	**LOST DOG** Find help fast!	**LONE WOLF** Could be overtaken	**ANKLE BITER** Annoying to cyberthieves	**SAINT BERNARD** On the ready	**GERMAN SHEPARD** Serious security!

www.planetmagpie.com