Essential Cyber Hygiene

4 Keys to a Strong Defense

STEP 01

Enabling Multi-Factor Authentication

MFA adds a vital layer of security to all logins. In most cases, a hacker can't breach an account protected by MFA even if the cyber crook has the password. MFA can block 99.9% of attempted account compromise attacks.

STEP 02

Strong Passwords & Password Managers

Always use strong, unique passwords for each account. Avoid easily guessable information like birthdays or names. Set strong password enforcement rules within your organization. This requires a strong password before it's accepted in a system.

STEP 03

Updating Software

Outdated software creates vulnerabilities that cyber-criminals can exploit. Regularly update operating systems, applications, and firmware to ensure the latest security patches are in place. Automating updates is a good way to ensure they're done promptly. Companies can use endpoint device managers to handle updates across all employee devices.

STEP 04

Recognizing & Reporting Phishing

Train your team to identify and report phishing emails, suspicious links, and unsolicited attachments. Verify the sender's email address and never provide sensitive information unless certain of the recipient's authenticity.

Turn Key Solutions
225-751-4444 www.turnkeysol.com