DIRECTIVE TECHNOLOGY

CYBERSECURITY TIP SHEET

Safe Password Dos and Don'ts

Build credentials that criminals can't crack

Why Passwords Still Matter

Stolen and reused passwords are behind the majority of data breaches. Even with multi-factor authentication in place, weak passwords give attackers a foothold they can use to harvest more credentials, send phishing emails from your domain, or move laterally through your network.

Do

- Use passphrases of at least 14 characters — four random words is a good start
- Use a password manager so every account gets a unique, generated password
- Turn on multi-factor authentication everywhere it is offered
- Change a password immediately if you suspect it was exposed
- Use biometrics or hardware security keys for your most sensitive accounts

Don't

- Reuse the same password across work and personal accounts
- Use family names, birthdays, pet names, or anything on your social media
- Store passwords in browsers on shared computers
- Email, text, or Slack passwords to coworkers — share via your password manager
- Write passwords on sticky notes near your monitor

How Attackers Crack Passwords

Modern hardware can guess billions of passwords per second. An eight-character password using only lowercase letters falls in seconds. A 14-character passphrase with mixed words and numbers can take centuries. Length beats complexity — focus on phrases that are long, memorable, and unique.

Have You Been Breached?

Billions of stolen credentials are circulating on the dark web right now. Directive Technology offers continuous dark web monitoring that alerts you the moment your business credentials appear in a known breach so you can rotate them before they are abused.