Cybersecurity Driver's Ed.

Operating Behaviors Bound for a Breach

STAY ALERT

DO

- Lock your computer when you step away or when you leave the office for the night
- Report a lost or stolen device to your IT department immediately

DON'T

- Leave sensitive information (logins, customer data, legal documents) on your desk or workspace
- Send any account information, like usernames or passwords, via unencrypted email

DRIVE DEFENSIVELY

DO

- Verify the identity of those that are requesting you to share sensitive company information
- Look for any confidential information that could be visible via screen-sharing prior to conference calls

DON'T

- Let an unknown person into your workplace because they "forgot their access card", ever
- Allow an outside vendor determine what "good" security is for your company, without any internal involvement

AVOID RISKY SHORTCUTS

DO

- Use a managed, protected personal device when accessing your company's private network(s)

DON'T

- Log in to guest networks with your work laptop/system, without network protection installed

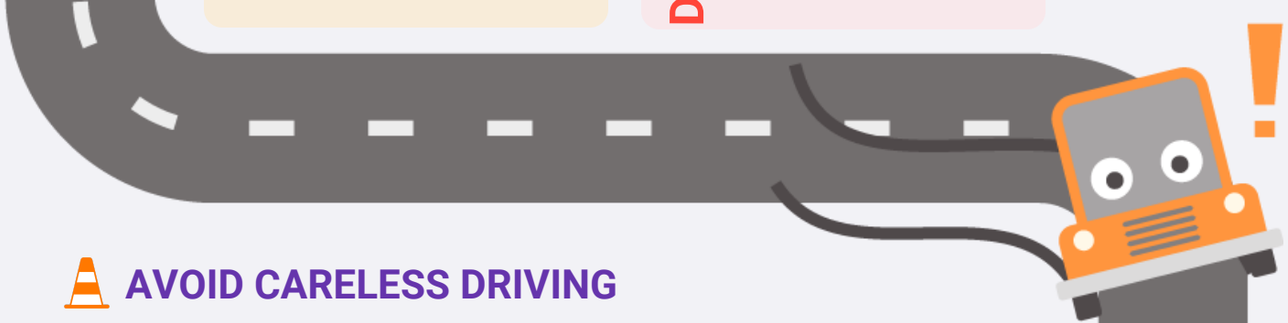
PAY ATTENTION TO SIGNALS

DO

- Update endpoint protection software, virus definitions, or security patches

DON'T

- Turn off auto-updating for your endpoint protection software to save time



AVOID CARELESS DRIVING

DO

- Use strong passwords for company resources
- Use secret questions that are not easily found online about you (mother's maiden name, pet's name, favorite band)

DON'T

- Reuse personal passwords for work logins
- Give others your login information
- Substitute "3" for an "e", "@ " for an "a" or other similar tactics to meet password requirements
- Keep a password file on your work computer or SaaS storage with all of your logins