

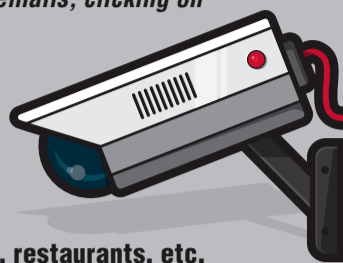
10 THINGS YOU CAN DO TO INCREASE PASSWORD SECURITY



ALWAYS KEEP INFORMATION SECURITY TOP-OF-MIND

HERE ARE A FEW EXAMPLES OF THE WAYS CYBER CRIMINALS OBTAIN PASSWORDS:

- * **Phishing** (also known as social engineering) - A technique cyber criminals use to trick users into revealing log-in information over the phone or in an email; resetting passwords through links to counterfeit website pages; providing sensitive information in response to fake emails; clicking on links to install malware; and/or downloading fake attachments.
- * **Shoulder Surfing** - Watching you enter your password or using a cellphone (or even a hidden camera) to record password entry.
- * **Guessing** - Sometimes people try commonly used passwords or use publicly available personal information to gain access to your private accounts.
- * **Intercepting passwords** over unsecure Wi-Fi at airports, coffee shops, hotels, restaurants, etc.
- * **Installing physical key loggers** or key logging software on devices.
- * **Searching devices and networks** for unencrypted passwords.
- * **Computerized decryption** - Techniques trying every possible combination of numbers, letters, and special characters until a password is discovered (also known as Brute Force Attacks).



CHANGE DEFAULT ADMINISTRATOR PASSWORDS

POINT-OF-SALES (POS) TERMINALS, SPECIALIZED HARDWARE, DESKTOPS, LAPTOPS, TABLETS, SMARTPHONES, SOFTWARE, ROUTERS, SWITCHES, ETC. are shipped from the factory with default administrator passwords installed in order to provide technical support remotely. But in the rush to use new hardware and software, users sometimes overlook default administrator passwords and neglect to change them. In other cases, default user-ids and passwords may be knowingly left in place to allow authorized third parties—consultants, contractors, Managed Service Providers, VARs—to provide technical support remotely. Recommended Best Practice is to change default administrator passwords IMMEDIATELY upon installation for all electronic devices at work and at home.

NOTE: Routers, switches, and point-of-sales terminals are particularly vulnerable to those with malicious intent.



USE UNIQUE PASSWORDS FOR CRITICAL APPLICATIONS

PASSWORDS KEEP INFORMATION PRIVATE AND FINANCIAL ACCOUNTS SECURE BY PREVENTING UNAUTHORIZED ACCESS

Using the same password for business and personal accounts is similar to using the same key for one's car, house, and office. Using the same password for multiple accounts makes it easy for cyber criminals to compromise one password to gain access to all of your accounts with the same password.

PASSWORDS ARE PRIVATE; DON'T SHARE YOUR PASSWORDS WITH ANYONE

PASSWORDS MUST BE TREATED AS PRIVATE, CONFIDENTIAL INFORMATION, not to be shared with anyone, *including coworkers*. This ensures company information is only viewed by those with authorized access and protects you from the bearing responsibility for the mistakes of others.

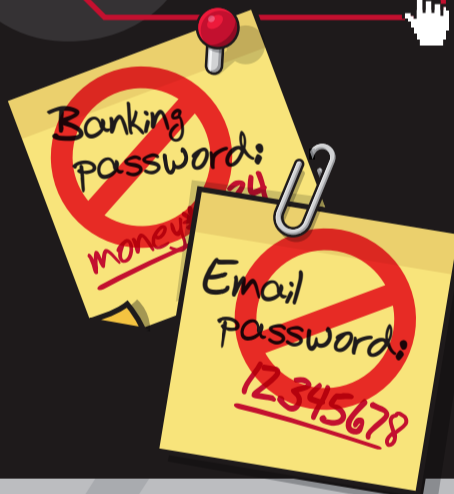


USE COMPANY APPROVED TECHNICAL SOLUTIONS FOR SECURE PASSWORD MANAGEMENT

AS WE RELY MORE AND MORE ON TECHNOLOGY, WE MUST REMEMBER, STORE, AND OTHERWISE KEEP TRACK OF DOZENS OF PASSWORDS. THIS SOMETIMES LEADS TO RISKY BEHAVIORS.

- * **DO NOT** - Write passwords down on "sticky notes," etc.
- * **DO NOT** - Store passwords on hard drives in unencrypted files.
- * **DO NOT** - Use easy-to-guess passwords.
- * **DO NOT** - Create predictable password strategies.
- * **DO NOT** - Employ the same passwords for multiple sites.
- * **DO NOT** - Log-in to accounts through major companies (Google, Facebook, Twitter, etc.)
- * **DO NOT** - Log in automatically, i.e., using "Remember My Password."
- * **DO NOT** - Reset passwords at each log-in.
- * **DO NOT** - Forget to log out at the end of each session.

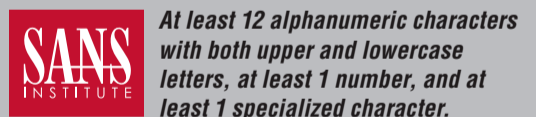
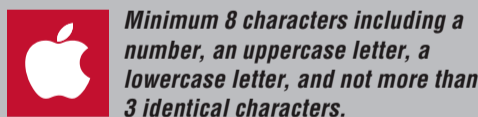
Recommended Best Practice is to use company approved technical solutions for securely remembering and storing your passwords, such as single sign-on, password managers, access cards, and/or biometrics.



CREATE STRONG PASSWORDS

PASSWORD COMPLEXITY CORRELATES DIRECTLY WITH PASSWORD SECURITY

While there is a wide variety of opinions over what constitutes a strong password, here are suggestions from 3 respected sources:



CHANGE YOUR PASSWORDS REGULARLY

The longer a password is used, the higher the chance it will be stolen or guessed. Recommended Best Practice is to change your password regularly

EVERY 90 TO 180 DAYS

and immediately upon suspicion or detection of a breach.



USE REAL-TIME PROTECTIVE MONITORING

WHETHER AT WORK OR AT HOME, KEEP YOUR OPERATING SYSTEM AND BROWSER UPDATED

Use firewalls, anti-virus, and anti-spyware software such as McAfee®, Norton®, Kaspersky®, Windows Defender, etc. for real-time protective monitoring. Heed all alerts, suspicious activity, and signals of intrusions.



SEARCH EQUIPMENT REGULARLY FOR PASSWORD INFORMATION STORED IN PLAIN TEXT

ONLY STORE ENCRYPTED PASSWORDS ON YOUR ELECTRONIC DEVICES

- * **DO NOT** send unencrypted passwords in emails.
- * **DO NOT** store unencrypted passwords in files, on company servers, in the cloud or on mobile devices.



ROUTINELY CHANGE PASSWORDS WHEN YOU CHANGE OR DISPOSE OF COMPUTING DEVICES



REMOVE ALL INFORMATION FROM COMPUTING DEVICES PRIOR TO DISPOSAL

And since many devices store passwords, take the added step of immediately changing your passwords on the replacement device.