People don't come naturally to passwords, and resist making passwords actually effective. Adopting good password practices can help your organization not fall victim to criminals taking your money.

11 WAYS
TO IMPROVE PASSWORD PRACTICES

1. **Passwords need to be unique to each account** (i.e. the password at Microsoft is not the same as at Google – so one criminal breach doesn't expose more than one account)
2. **Passwords cannot be reused** (i.e. don't recycle no-longer-used passwords – those might have been breached)
3. **Passwords cannot be made of letter/number/symbol substitutions** (i.e. shell written as 5he!! – criminals' software now guesses these substitutions easily)
4. **Passwords cannot be based on user names or email addresses** (too easy for software to guess)
5. **Passwords are not considered new when a password is slightly changed** (i.e. like adding a 1 or ! – criminals' software again)
6. **Passwords must be of a certain length** (to keep ahead of password-cracking programs, 2024 advice is at least fifteen characters)
7. **Passwords should be stored in either**
   a strong-password-protected and encrypted digital way (like in a password manager) or in a secure physical way – like in a locked file cabinet
8. **Password sharing is not a good idea** – if necessary limit it to encrypted methods (like in an encrypted PDF)
9. **Consider password manager software** (like LastPass, BitWarden, 1Password, etc.) that creates and stores strong, complex passwords (some products allow admin oversight of employee passwords)
10. **Check if your email address has been breached** at haveibeenpwned.com or through dark web monitoring that can watch if any email address from your domain has been in a breach
11. **Turn on multifactor authentication (MFA) whenever possible** (MFA makes your employees confirm their identity in more than one way [like with both an email address and an authenticator app on a phone] to cut the risks of exposed passwords)

Online resources to help generate good passwords:
Steve Gibson's password generator is at grc.com/passwords.htm
Univ. of Illinois has a password-strength checker at uic.edu/apps/strong-password

bryleysystems™

Bryley • Business Continuity through Managed IT
Bryley Systems Inc, 200 Union St, Clinton, MA 01510 • 978.562.6077 • Bryley.com