1. Keep passwords a secret, even from tech support. No one else should have your password. Ever.
2. Make it more complicated. Don’t use simple words or personal information.
3. The longer the better. Passwords become harder to crack the longer they are.
4. Use a passphrase instead. It’s much harder to hack “IAteA$10Hotdog” than “SummerFun18.”
5. Don’t duplicate passwords. Use a unique password for each site, and don’t simply add another number to end of a single password.
6. Change passwords every 60-90 days. This is especially true for sites with sensitive information.
7. If you think an account has been compromised, change your password immediately. Also check other accounts for suspicious activity.
8. Make security question answers hard to guess and vary your questions/answers so that you aren’t duplicating security information.
9. Implement additional security features, such as two-step authentication.
10. Have password procedures for your entire firm. Any employee can be a weak link in security.

Secure Password Checklist

- Use longer passwords, preferably a passphrase (12 or more characters.)
- Use a combination of letters, special characters, and numbers.
- Avoid using names, dates, or words found in the dictionary.
- Never share your password.
- Do not write your password down.
- If you think a password is compromised, change it immediately.