CREATING STRONG PASSWORDS

Kevin Mitnick Security Awareness Training

"It's important to keep malware (malicious software) off your computer so hackers cannot intercept your passwords. Even if your passwords are very strong and hard to guess, malware can still allow a hacker to get them."

–Kevin Mitnick

Kevin Mitnick's 10 Rules for Stronger Passwords

Always use strong passwords on the internet. A strong password is one that is hard for someone else to guess.

1. Don't tell your passwords to anyone, even tech support people who may ask you for them. *Nobody* should ask for your password, and you should never give your password to anyone.
2. Don't use simple dictionary words or pets' or people's names for your password. And avoid things like your zip code or key dates like a birthday or an anniversary.
3. Use passwords that are at least 12 characters long; however, those are still easy to crack if an attacker gets into your network. If you want to be super safe, use 20 characters. And don't write them down where they can be easily found.
4. It's actually easier and more secure to create a passphrase instead of a password. A passphrase is a few nonsense words like *$3 for the pirate hat* or *Betty was smoking tires and playing tuna fish*.
5. Use a different password for each website. And don't use simple patterns like *password1*, *password2*, *password3* for different sites—those are too easy to guess.
6. Change your passwords for sensitive websites, like online banking, every 60-90 days, and, like Rule 5, do not use easy-to-guess patterns when you change them.
7. If you think your password may have been compromised, change it immediately and check your other websites for any signs of misuse, starting with your online banking site!
8. Sometimes websites ask you to enter the answer for a security question that you can use if you forget your password. Make sure that your answer to that security question is just as hard to guess as your password. This answer should not be used anywhere else.
9. Use extra security features, such as stronger forms of authentication, everywhere you can. For example, a site may offer an option to use Google Authenticator, which is an app that generates a new six-digit number every minute as a "second password." That is a good security feature, so use it! Sites also sometimes offer to send you a code via a text message. To log in to your account, you need both your password and the code. That's less secure than the Google Authenticator app on your phone but better than nothing.
10. Use the password procedures that your organization requires you to use, and consider using a password manager at home. These products make it much easier to have strong, unique passwords on all of your accounts. There are also online password generators that create hard-to-guess passwords—for example, www.passwordsgenerator.net.

KnowBe4
Human error. Conquered.

Tips for Password Security

- ☐ Keep your passwords private—never share a password with anyone else.
- ☐ Do not write down your passwords.
- ☐ Use passwords of at least 12 characters or more (longer is better).
- ☐ Use a combination of uppercase letters, lowercase letters, numbers, and special characters (for example, !, @, &, %, +) in all passwords.
- ☐ Avoid using people's or pets' names or words found in the dictionary. It's also best to avoid using key dates (birthdays, anniversaries, etc.).
- ☐ Substituting look-alike characters for letters or numbers is no longer sufficient (for example, "Password" and "P@ssw0rd").
- ☐ A strong password should look like a series of random characters.
- ☐ On the web, if you think your password may have been compromised, change it at once and then check your website accounts for misuse. At work, change your password at once, and then call your company's IT security help desk.

Password Management Software Products

In the office, your organization may not be able to use these, but for the house, there are good password manager software products on the market today. Some are free; none are very expensive. Using one of these products, you can create truly random, very long, and unique passwords for each site, and because the software will remember them for you, you never have to worry about what your password is. Your password manager will store and encrypt the passwords for you and log you in automatically. You will have vastly improved security, with only one master password to remember.

How to Create a Strong, Complex Password

Here's a way to make a strong password that's very hard to crack:

Follow These Steps	Example
1. Think of a phrase or sentence with at least eight words. It should be something easy for you to remember but hard for someone who knows you to guess. It could be a line from a favorite poem, story, movie, song lyric, or quotation you like.	**I Want To Put A Dent In The Universe**
2. Remove all but the first letter of each word in your phrase.	**IWTPADITU**
3. Replace several of the uppercase letters with lowercase ones at random.	**iWtpADitU**
4. Now substitute a number for at least one of the letters. (Here we've changed the lowercase "i" to the numeral "1.")	**iWtpAD1tU**
5. Finally, use special characters ($, &, +, !, @) to replace a letter or two—preferably a letter that is repeated in the phrase. You can also add an extra character to the mix. (Here we've replaced the "t" with "+" and added an exclamation point at the end.)	**iW+pAD1tU!**

This guideline on creating strong passwords is just a small section of the Kevin Mitnick Security Awareness Training. For more information and to train all employees, please visit **www.KnowBe4.com**.