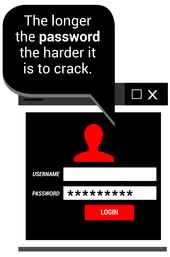
Five Steps to Create a Secure Password

(That You'll Actually Remember)

Let's Start with *The Basics*



Consider a **12 character** password or longer.
(Shoot for 20 characters!)

Do **NOT** choose your pet's name, birthday, address, family members names, etc.

Use **variations** on capitalization, spelling, numbers, and punctuation.

Use mixed-case letters, numbers and symbols **(#, $, !, %, *)**

Use a **different** password for every account that you have.

Let's Create a Secure Password in Five Easy Steps

STEP 1

Choose a sentence or a phrase with eight or more words. This can be easy for you to remember, but hard for someone to guess even if they know you well. Consider catchphrases from a movie or book, a poem you like, a line from your favorite song, or even a motivational quote.

Example: *Toto, I've got a feeling we're not in Kansas anymore.*

STEP 2

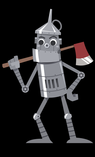
Now, remove all the letters except for the first in every word.

Example: *TIGAFWNIKA*

STEP 3

Next, randomly replace some of your uppercase letters with lowercase ones.

Example: *TIGaFwNiKA*



STEP 4

Replace a letter with a number. In our example, we replaced the "I" with the number "1."

Example: *T1GaFwNiKA*

STEP 5

Now mix in a special character to either replace a letter or just be randomly tossed into the mix. In our example, we added a comma after the "T "and an exclamation point at the end of the password.

Example: *T,1GaFwNiKA!*

EIGHT Key Takeaways for Strong Password Creation

1. **No sharing of passwords**
2. **Passwords should be between 12 to 20 characters**
3. **Combine upper and lowercase letters, special characters,and numbers in passwords**
4. **Do not store your passwords in your notes physically or virtually**
5. **Don't use easily guessed combinations such as loved ones' names, birthdates, or anniversaries**
6. **Your password should look like a series of random characters**
7. **Substituting look-alike characters for letters or numbers is no longer sufficient (for example, "Password" and "P@ssw0rd")**
8. **Take quick action if you think you've been compromised**

Tips for EXTRA Security

- Use a **Password Management** Tool
- Consider making your **Security Challenge Questions** as complex as the password.
- **Layer Your Security** with multi-factor authentication, text message prompts, or Google Authenticator.

React Quickly to Compromise

If you suddenly have an issue logging in to a site (i.e. "password not recognized"), you have probably been compromised. Change that password immediately and check all other applications for compromise. It's a safer bet to proactively change all your passwords if you suspect one site or application has been compromised.

Integris.

www.IntegrisIT.com