

CYBERSECURITY

What Makes a Strong Password

The frustration of a forgotten password can be just **TOO MUCH TO BEAR.** Why not go with "charles15" or "mypassword"?

BECAUSE CYBERCRIME IS SO PREVALENT.

If you want your bank account to still have your money in the morning, you'd better **STRENGTHEN YOUR PASSWORD.**

Find out what makes a secure password, different techniques to create them, how to make them memorable, and what were some of the worst passwords of the past year!

Avoid a Weak Password...

DON'T REUSE PASSWORDS
for at least a year.

DON'T
use a duplicated good password
example—create your own.

DON'T USE THE SAME PASSWORDS
for multiple accounts.

DON'T USE PERSONAL INFORMATION
(name, birth date, etc.)

DON'T USE
DICTIONARY WORDS

DON'T use keyboard patterns
QWERTY
or sequential numbers
12345

DON'T make your password all numbers, uppercase letters or lowercase letters
MIX IT UP

DON'T use repeating characters
222TT

Tips to Create a Strong Password

Include punctuation marks and/or numbers

Mix Capital and lowercase letters

Make an acronym from a phrase

Include phonetic replacements, such as
LUV 2 LAF
for
LOVE TO LAUGH

Be creative with these—password hack software can detect them

Try a **PASSPHRASE**

Use substitutions, like the number zero for the letter 'O' or '\$' for the letter 'S'

What's a Passphrase?

A passphrase is typically **20 TO 30 CHARACTERS**

THREE OR MORE words is **IDEAL**

Employ characteristics of a **STRONG PASSWORD**—mixed cases, symbols, numbers, acronyms and more

Switch the **ORDER OF WORDS** in the phrase for **MAXIMUM SECURITY**

Password Strength Tools

If you're unsure about the hackability of your password, run it through a strength test.

MICROSOFT
HOW SECURE IS MY PASSWORD,
and many other places offer these **FREE**

Password Generators

If you can't come up with a password (or just don't want to), use a **PASSWORD GENERATOR**

The generator will select from
LETTERS
NUMBERS
SYMBOLS

The number of possibilities for an 8-character password:
645 753 531 245 761
Wolfram|Alpha, PC Tools, GoodPassword and more offer these free.

Tips to Remember Passwords

PASSPHRASES are often easier to remember.

Believe it or not, a random string of words can be easier than an acronym or sequence of numbers

Keep a list of password reminders—instead of writing down the password itself, use a prompt

For example, "Your childhood cat" would help you remember **4U4YthEmAgnificEnt**

LastPass, KeePass, Roboform and 1Password keep multiple passwords accessible and secure with one password

These can often be transferred onto mobile devices or USBs so they're with you at all times

What Makes Password Hacks Easy?

50% the chances that a password has at least one **VOWEL**

Numbers are usually **1 OR 2** and are placed at the end

50000-150000—the average vocabulary of a person, and the words likely to appear in a password

Capital letters are usually at the **BEGINNING** and are followed by a vowel

Women use **PERSONAL NAMES** for passwords frequently.

Men use their **HOBBIES** for passwords frequently.

Most common symbols: **~!@#%&?**

Keep Your Password Secure

NEVER reveal your password to **ANYONE**

Never write your password down—and **IF YOU INSIST** keep it hidden and far from your computer.

TEST AND CHANGE your password **REGULARLY**

Be doubtful of links asking for log-ins, passwords or personal information. If you're unsure the site is legitimate, type in the URL manually **BEFORE** entering account information.

Always **LOG OFF** especially if your device is on around others. Password steals and changes can happen instantly.

Don't type your password into public computers (at libraries, etc.)—**MALWARE** may steal them.

10 Worst Passwords of 2011

PASSWORD	123456	12345678	QWERTY	ABC123
MONKEY	1234567	LETMEIN	TRUSTNO1	DRAGON

Password Statistics

25 number of online accounts for average internet user

6.5 number of passwords for average internet user

2/3 of users have only 1 or 2 passwords

3.1 MONTHS average time between changing passwords

Sources

<http://www.microsoft.com/security/online-privacy/passwords-create.aspx>
<http://www.movements.org/how-to/entry/how-to-create-strong-passwords-splashdata.html>
http://help.yahoo.com/kb/index?locale=en_US&y=PROD_ACCT&page=content&id=SLN3012
<https://accounts.google.com/PasswordHelp>
<http://mytechnoguide.com/2011/02/interesting-password-statistics/>
<http://www.uc.edu/infosec/password/chooseapassword.html>