

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION



DTI eSecurity News — Password Picnic

Passwords Again?



We understand, everyone gets tired of the safe, strong, password sermon. However, if there's one simple step you can take on the road to cyber safety, it's making sure that your passwords don't win the "most likely to be guessed" award. Read on for some helpful tips and timesavers.

Password Planning

Take a mental inventory of your current usernames and passwords. Every time you login to a new site, jot it down if you need to, by site name, username, password and categorize it by risk level. Don't do this online and take great care to safeguard your list.

What is risk level? In this case it's a way of quantifying the sites that you regularly visit based upon those that contain the largest amount of personal financial data. Think bank accounts, credit card accounts, mortgage and other loan payment sites. These are the highest risk sites; next comes high risk sites such as Amazon, eBay, Target, retail shopping sites that you use regularly. Moderate risk sites include social media, like Facebook, Twitter, etc.

Next, rank your sites by risk level. Give immediate attention to your high risk sites. Make sure that they have the strongest passwords and make the passwords different for each site to reduce your risk.

Now What? Password Ideas

Is your current password "Summer2015", or "Password1", or "12345678"? A hacker can crack those in *less than a minute*.

A strong password should be at least ten characters (12+ is better). Since 12 characters or more can be hard to remember, thinking about phrases can be easier. Here are some suggestions:

- **Song Title**
Use the first letter of each word in the title.
For example: "SirPaulLiveALDie1!" (Live and Let Die)
- **Favorite Thing**
My Favorite Thing = (fill in the blank)
For example: "MFT=HFSDayZ7" (my favorite thing equals hot fudge sundaes.)
- **Airport Code**
Frequent flyer? Use an airport code like ORD (O'Hare in Chicago) with a favorite word and number combination.

Tired of Keeping Track of Passwords?

Our favorite password tracking tool is Password Safe.
<http://passwordsafe.sourceforge.net/>

It runs locally, it's free, the file is encrypted, it's not as clumsy as thumb drives or paper logs, and you only have to remember one password - the combination to your password safe. It's easy to use both at work and at home.

It will take you 5 minutes to set it up. Why not give it a try?

Visit our [Cyber Security website](#) for previous issues of
eSecurity Newsletters

Questions or comments?
Email us at eSecurity@state.de.us

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

