TIPS & TRICKS

DADE COUNTY TECHNOLOGY

Week of April 7, 2014

Password Protected

Tons of information is now available online. Much of this information is protected with passwords. Just about everything has a password. Knowing that… how secure are your passwords?

Is your password on a sticky note posted to your monitor? Or on a piece of paper under your keyboard? Do you use the same password for your email, your network login, and your online access to your bank account? Is your password something that can be easily guessed (ie. pet's name, child's name, favorite movie or movie character, etc…)?

What makes a good (or bad) password? Here are some thoughts…

1. Avoid common names, dates, phone numbers, family member names, and other things easily associated with you. Try to make your password as meaningless and random as possible.
2. Avoid common words or phrases since they can easily be guessed by password cracking software. There is something called a "dictionary attack" that simply tries all the words found in its list of "real" words until it finally cracks your password.
3. Don't use your username as your password. And don't use the word *password* for your password.
4. Use a combination of uppercase letters, lowercase letters, numbers, and special characters by substituting characters in your password (ie. change password to pAs$w0rd). It may take a while to remember it but soon it will become second nature to type it without thinking about it.
5. Make your password is something you will remember all by yourself so there is no need to write it down anywhere. And don't let your computer "remember" your password. Don't be lazy… type it in each time.
6. Don't use naturally occurring keyboard sequences like *qwerty* or *12345678*.
7. Try to make it 8 or more characters long (the longer the better). I have some passwords for my online web sites that just under 20 characters long and incorporate uppercase

letters, lowercase letters, and numbers. Bet you can't guess them! :)
8. Avoid using the same password at different locations (ie. web sites, voicemail, bank accounts, etc…)
9. Plan on changing your password often.

Here's my story of being hacked:

Every now and then I noticed that in my personal email that I was receiving what appeared to just be SPAM making references to my iTunes account… thanking me for my purchase. I thought there was nothing to the emails… that maybe I was getting SPAM in the hopes that I would reply with some pertinent information. Then one day when I just happened to log into my iTunes account I noticed that it said I have downloaded the song, "Don't Stop Believin'" by *Journey*. I knew without a doubt that all I had downloaded from iTunes for quite a while was soundtracks for me my girls to sing with at church. So I looked at the history and found some other interesting downloads that I had supposedly made. As a matter of fact, when I looked at my email account associated with PayPal and iTunes I saw where several phone apps were scheduled to be downloaded… costing enough to bounce my account at the local bank that was associated with the PayPal account. I contacted PayPal and they said that I should contact the bank and have them deny payment. I did this and then tried to contact iTunes (with no luck). Because my bank denied payment through PayPal, PayPal deactivated my account. I ended up killing off my iTunes account and signing back up with a different email account. I finally got my PayPal account reinstated. I altered my passwords for not only PayPal and iTunes but for all of my online accounts making them incredibly long and complicated. Remember up top where I said that I had passwords that were just under 20 characters of mixed uppercase letters, lowercase letters, and numbers? That's how I have those protected now.

Please send any questions or comments about this installment of Tips & Tricks to technology@dadecs.org.