



COMPUTER AND TECHNOLOGY CONSULTING WITH A *PERSONAL* TOUCH

June 1, 2009 Newsletter

1. P@ssw0rD5
2. They don't need a Phishing license
3. About me and this newsletter

#####

1. P@ssw0rD5

The typical Netizen (Internet citizen) would be astonished at how much of their personal, and even confidential, information is available on the Internet. Obviously, the security of the information is not fully within the individual's control, but much of it is. Imagine how much chaos could be created if a malicious person gained control of your online accounts (email, credit cards, bank accounts, bills, etc.). This is why it's important to use strong passwords for every online account - or even on your computer itself if you have an untrustworthy roommate.

Here's what Google suggests:

- "- Be creative. Don't use words that can be found in a dictionary.
- Use at least six characters.
- Don't use a password that you have used elsewhere.
- Don't use keyboard patterns (asdf) or sequential numbers (1234).
- Create an acronym. Don't use a common one, like NASA or SCUBA. Don't make your password solely an acronym, combine it with numbers and punctuation marks.
- Include punctuation marks. Mix capital and lowercase letters. Include numbers.
- Include similar looking substitutions, such as the number zero for the letter 'O' or \$ for the letter 'S'.
- Include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh.'
- Don't make your password all numbers, all uppercase letters, or all lowercase letters.
- Find ways of collecting random letters and numbers, such as opening books, looking at license plates or taking the third letter from the first ten words you see.
- Don't use repeating characters (aa11).
- Don't use a password that is listed as an example of how to pick a good password.

Tips for keeping your password secure:

- Never tell anyone your password. Don't write it down.
- Never send your password by email.
- Periodically change your password."

Implementing even a couple of those suggestions will help tremendously. So let's say you play by the rules, and your email password is now 'H7#djhsUH*3'; how in the heck are you supposed to remember that? Let me introduce you to a type of software called Passwords Databases. These are encrypted, password-protected databases that you can easily create to store all your passwords. You'll create a master password (that you must memorize) that gives you access to your vault of passwords. Many of these password keepers are free and easy to use, and many will automatically paste the requested password in to the box on the website you're trying to log in to. Just be sure to choose a reputable password database manager.

P.S. Don't use 'P@ssw0rD5' either.

Related reading:

<http://www.google.com/support/calendar/bin/answer.py?hl=en&answer=37053>
<http://netsecurity.about.com/od/newsandeditorial1/a/storepasswords.htm>

#####

2. They don't need a Phishing license

Aside from guessing or cracking your password, another very common way criminals gain access to your accounts is by Phishing. According to Wikipedia, phishing is "the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication." So let's switch back to simple English terms. Phishing is when you receive an email that *appears* to be from an organization, telling you that something is wrong with your account and/or you need to log in to it. The email conveniently provides you with a link to the website and you type your username and now-strong password but for some reason you can't log in. BAM! The damage is already done. You have been duped in to giving up your confidential information.

These phony emails and corresponding website are designed very carefully and thoughtfully to look exactly like the real thing. The criminals want you to not even think twice about the legitimacy of them, and then lead you in to their wolves den. Now that you have typed your username and password in to their bogus site, they record it and try to gain access to your actual accounts.

So in the future, if you receive an email from any online service or financial institution, ask yourself a couple questions instead of clicking any links within the email. First, "do I really have an account with these people?". If not, delete the email and pat yourself on the back for spotting a forgery. If you do have an account, then the second question is "what is this organization's phone number?". That's right, you're next step is to call them and straighten it out on the phone. Never respond to or click on any email like this. If there is a real problem with an actual account you have, you'll want to take care of it by phone. Manually go on the organization's website and find their phone number.

Related reading:
<http://en.wikipedia.org/wiki/Phishing>

3. About me and this newsletter

Lee Abrams is an IT professional in the Philadelphia area, and has over 8 years experience helping computer users and bringing valuable services to small businesses. People have come to rely on his experience, integrity and speedy service in a variety of situations, including computer, network and server installation and repairs (Windows and Apple OS X computers), website design and maintenance, consulting and coaching, PC disinfection and clean-up, and general technology services.

I write this newsletter as a value-added service to my clients as a way to help keep computer users abreast of the rapidly changing landscape. Please feel free to pass this on to anyone who you may feel this will be useful, but unaltered.

I would never lead you astray, so every website link in this newsletter has been visited by me and has been verified to be non-malicious at the time of writing.

Please note that all content within this correspondence does not carry any warranty or guarantee, neither written nor implied.

If you would like to read past newsletters, please visit <http://www.digitallee.net/archives.html>

I hate spam; everyone hates spam. I hope you don't consider this email spam. I respect your privacy and your wishes, so if you wish to not receive this newsletter any more, please reply to this email and indicate so. I promise you won't receive any more.

Computer and technology consulting
with a personal touch
www.DigitalLee.net