The INFormer—Security Edition

Volume 1, Issue 1 December 17, 2012

INtegrity First Corporation

How to Create a Safe Password

If your password is less than eight characters, there is a good chance that it can be hacked in less than five minutes by commercial software available to anyone! In fact, most of this software costs under five-hundred dollars. To avoid being exploited by this, remember these five tips:

(1) ***Don't use real words for your password*** – Do not use words or combinations of words from the English dictionary or any dictionary for that matter. Password cracking programs have algorithms that use lists of words and permutations of words to guess your password.

(2) ***Don't use your name, your spouse's name, or any other family member or pet's name as your password*** – This is one of the most common password types and the easiest to guess. Password cracking programs also have access to lists of millions of names, which they will use in their algorithms as well.

(3) ***Use at least twelve characters for your password*** – The longer your password is, the more resistant it is to being broken. Most people think that they cannot remember a password of that length, but there are multiple ways to form a memorable password.

(4) ***Form a memorable password*** – If you can remember a song lyric or a poem, you can remember a long password. Start with a phrase or lyric (containing at least twelve words) that you like, and then use the first letter or the last letter of each word as your password. Finally, substitute symbols and numbers for characters and/or phrases, such as "H&" for "hand" or "8" for "ate". It may look like texting, but it creates a stronger password.

Using a strong password will help keep your computer safe

(5) ***Use a combination of numbers, letters, and symbols for your password*** – Any password created should use uppercase characters, lowercase characters, numbers, and symbols, which will give you 90^{12} possibilities, which is a lot of combinations for a password cracker to guess, about two-hundred eighty-two sextillion possibilities to be exact.

4 Rules for Password Use

(1) Change your password at least once every three months – Remember, given enough time and enough resources, any password can be cracked. One way to overcome this issue is to change your password every one to three months and never on a straight schedule. This way, there is not an infinite amount of time available to guess your password.

(2) NEVER write your password down – This is one of the easiest ways for someone to steal your password. As soon as you leave your desk/office for the day, your password is available to anyone who may be in your building/house/office.

(3) NEVER give your password to anyone – You should never give out your password over the phone. Almost all tech support should never ask for your password, they should verify your information in a different way

(4) NEVER use the same password for multiple accounts – If one of your accounts is hacked, you do not want the hacker to have access to everything. Therefore, use different passwords for different accounts. If you think that you cannot remember all of them, there are multiple free programs available that will remember them for you. Check out KeePass for more details.

Inside this issue:

Special points of interest:

- Look for 5 tips for creating a Safe Password
- Learn the best practices for password use
- Secure-A-Day is offered by INF to advise on security risks

INtegrity First Corporation

3633 Poplar Avenue
Pittsburgh, PA 15234

Phone: 412.563.2106
Fax: 412.563.6109
Email: info@integrityfirstins.biz
Web: www.integrityfirstins.biz

Secure-A-Day

Secure-A-Day is a virtual walk-through of your typical day through the eyes of a security professional in your own office environment. We review typical security exposures found in the office, while away at meetings, and at home. For more information on this class, visit: http://integrityfirstins.biz/Home/SecureADayDetails.

This class is offered by Stacey Ivol. Stacey has her Bachelor of Engineering degree

from the University of South Carolina in Computer Engineering as well as her Masters of Science degree from Carnegie-Mellon University in Computer Engineering, with a focus on cryptography. She is the Vice President of the Privacy/Data Breach Unit for INF, Web Master for multiple companies and does security consulting for small businesses.

According to the Ponemon Institute, the average organizational cost for a data breach is $5.5 million and the average cost per stolen record is $194.

Privacy/Data Breach Insurance

Your company can take many security precautions, but it can never eliminate the element of human error or the persistence of hackers. Hence, there is a need for Privacy/Data Breach insurance. It covers you in the event of a breach, addressing both first- and third-party breach risks that are associated with retaining client data in any form as well as exposures that are created by e-business, the Internet, networks, and computers in your office. The term cyber liability is a bit of a misnomer, as this insurance applies not only to electronic media, but to paper files as well.

A data breach is any access/acquisition of data that threatens the privacy of personal information as stored by YOU as part of an aggregate of personal information stored by YOU and YOU believe that it has or will cause injury/loss.

ALL businesses should have Privacy/Data Breach Insurance, especially if they: are regulated by HIPPA laws, maintain/update a database with client information, complete financial transactions, or maintain a web presence, which may or may not include e-commerce. Additionally, these exposures are typically NOT covered under traditional insurance policies, so there is no pre-existing coverage.

According to the 2012 Data Breach Investigations Report by the Verizon RISK team, over 70% of all data breaches happened to companies with less than 100 employees. According to the report, small to medium companies have become the main target of hackers due to the low risk, high reward profile.

If your company has a breach, there are multiple requirements that you must follow:

In the state of Pennsylvania as per Pa. Statutes 73 § 43-2303, if you have a breach, you must notify the individuals that are affected via e-mail or regular mail. If the breach affects more than 1000 individuals, the nationwide credit reporting agencies must be notified. Depending upon the situation, state and federal law enforcement may need to be notified. In addition, you or a hired third-party, will have to determine the cause of the breach and to remedy said issue.

If you or your company is interested in a quote for Privacy/Data Breach insurance, please contact Stacey Ivol at INtegrity First Corporation for more details. It is very easy to get a quote, as the application is 4 questions. For most companies, the price of a good laptop will buy you a policy and peace of mind.