BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

March 2015 | Briefing 3

PASSWORDS ARE THE WEAKEST LINK

HOW MANY ONLINE ACCOUNTS DO YOU HAVE?

If you are like most people, you have between 30 and 35 unique online accounts that require a username and a password to access. These accounts include work email and network access credentials, two to four personal email accounts, banking, credit card, home insurance, health insurance, brokerage, social sites like Twitter, Facebook, Instagram, Pinterest, and Linked-In, photo sites like Flickr, auction sites like Craigslist and eBay, entertainment sites, like Hulu and Netflix, college or university alumni sites, wireless networks and others.

HOW MANY PASSWORD SECURE THOSE ACCOUNTS?

Again, if you are like most people you have one or two standard passwords that protect your personal data from prying eyes. Maybe you have a couple of keywords and a couple of numeric special character strings that you mix and match. Whatever your strategy, you feel protected.

USER NAMES AND PASSWORDS ARE ALMOST ALWAYS THE WEAKEST LINK IN A SECURITY SCHEME

In today's world, once a thief uncovers or steals one of your username/password combinations, they quickly try them on all the standard email and social sites. And if you are like most people – reusing usernames and passwords across sites - the thief will gain access to several of them. When a thief has access to your account – what do they do first? They lock you out by changing the password! Suddenly an unknown, malicious third party has access to your online identity, and can masquerade as you to your friends, colleagues, and the public.

PASSWORD THEFT IS BIG BUSINESS

Because stolen usernames/passwords and other personal identifiable information (PII) are sold on the black market, password cracking has become big business. Today's password crackers are highly trained engineers who go to an office every day, and use very best hardware and software tools. They can try millions of combinations per second, and use powerful decryption techniques to guess or discover passwords. In a recent WIRED magazine test, a computer expert using off-the-shelf hardware was able to decode more than 90% of 15,000 encrypted passwords in less than one day. Another expert, using specialized hardware, was able to decode 82% of those passwords in less than one hour.

RECENT BLACK MARKET PRICES

HEALTH RECORD ID/PASSWORD - **$8-10**

ITUNES - **$8**

FEDEX.COM, CONTINENTAL.COM & UNITED.COM - **$6** GODADDY.COM,

ATT.COM, SPRINT.COM, VERIZONWIRELESS.COM & TMOBILE.COM - **$4**

FACEBOOK & TWITTER - **$2.50**

DELL.COM, OVERSTOCK.COM, WALMART.COM, TESCO.COM, BESTBUY.COM & TARGET.COM - **$1-3**

WHAT MAKES A GOOD PASSWORD?

Basically there is a simple answer to this one – the longer your password is, the harder it will be to crack. There are other password creation guidelines which are commonly used:

DO use a minimum of 10 characters (more is better)

DO use upper case, lower case numbers and special characters

DO NOT use only dictionary words - use some slang, or intentional misspellings, foreign words

DO NOT use family birthdays, addresses, phone numbers or SSNs

In 2014, news broke of a group of Russian hackers who had successfully stolen over 1-billion user ID and password combinations from weakly secured websites.

PASS PHRASE PASSWORDS

A popular password technique involves using a long pass phrase instead of a shorter text string.

Most experts agree, a 4-word phrase – correct horse battery staple – is probably a harder password to crack than a 10-character random password. And by adding – capital letters, spaces, underscores, and a few special characters to that very same four word phrase: – you will create a password that will be virtually impregnable. Just by adding spaces in between the words, you've made the password three characters longer, and exponentially harder to crack using brute force.

RULE-BASED PASSWORDS

Change your approach. Don't try to imagine a password – synthesize it. Use a rule to create a password by using a combination of inputs. Here is an approach based on using a popular song and the service for which you are creating a password, you can easily adapt it to use other information to seed the password.

1) Use a popular song to create a base string. To keep things simple we'll use a song that everyone knows – Happy Birthday To You.

2) Now take the first letters of each of the words in the song's first phrase – HBTY. Put them in lower case: **hbty**.

3) Now take the name of the domain or site for which you are creating a password. Let's pretend we are making a password for a Gmail account: GMAIL.

Interleave the letters of the domain into the seed. **hGbMtAyIL**.

4) Now turn every third letter into its alphabetical number (A1, B=2, C=3) **hG2Mt1yl12**.

Finally, change every other digit to the special character on the same key of a standard keyboard 1=!, 2=@, 3=#, etc…

5) hG@Mt1yl!2.

Eureka!– A rule-based password for your Gmail account. It isn't a random password – it's a rule-based password, and only you know the rule. If you use this rule for your CNET account or your Neflix account you will get completely different passwords: CNET = **hC@Nt5yT** ; Netflix = **hN@Et2)yF1)IX**.

EASY TO REMEMBER - HARD TO CRACK - UNIQUE PASSWORDS FOR EACH ACCOUNT?

You know that to ensure your online safety, you should have passwords that are hard to crack – long, strong passwords that utilize some or all of the techniques outlined in this Brief. But you also know you should make a unique password for each account that you log into.

But how do you create a lot of long strong passwords and remember them?

LONGER IS BETTER

(average time to crack a random password)

10 character password 5 days

11 character password 2 months

12 character password 3 years

13 character password 170,000 years

USE A PASSWORD MANAGER

To help you keep your online accounts more secure, and to simplify the process of maintaining a robust array of lengthy, hard-to-crack passwords, a password manager will do the hard work of generating a long randomized password for each online account you maintain, and save then, in encrypted form, safely on your computer. A When you visit a password protected site, the password manager provides the site with its unique password and you log in. With a password manager, you don't have to rely on a single password you use on multiple accounts; each site can have its own unique password. And the site-specific passwords no longer have to be easy to remember – the password manager generates the passwords and saves them for you. Instead, you use a master password, from a trusted machine, to access the secure encrypted list of site-specific passwords held by your password manager.

POPULAR PASSWORD MANAGERS

Here is a listing of popular password managers*; many of these providers offer both free and premium versions of their tools, with differing capabilities.

LastPass **** · keeper · Sticky Password · PasswordBox · INTUITIVE PASSWORD · dashlane · Norton · RoboForm

*Increasingly, browsers like Google Chrome offer you the option to save passwords for each site, just as a dedicated password manager might. Some users find this convenient, but generally, without the password generating features of a true password manager, saving passwords in a browser often perpetuates the recycled password problem.

TWO-FACTOR AUTHENTICATION!

Two-factor authentication has been around for years, but recently, Google began offering two-factor authentication for Gmail and Google users. Today, any other sites and password managers now offer two-factor-authorization. (see sidebar)

Two-factor authentication provides powerful protection against unauthorized account access. With it, even if a hacker should gain access to your user name and password, they will be unable to access your account without access to your phone or one of your previously designated trusted devices.

The basic principle behind two-factor authentication is this – to gain access to your account, you have to provide two pieces of information; something you know (your user name and password) plus something you have, a special numerical string (one time, or one that changes frequently) is sent to you by some other means, usually a SMS text or voice message.

GET TWO-FACTOR AUTHENTICATION HERE

If an account you use offers you a two-factor authentication option, you should enable it.

- Google/Gmail
- Apple
- Facebook
- Twitter
- Dropbox
- Evernote
- PayPal
- Steam
- Microsoft Accounts
- Yahoo! Mail
- Amazon Web Services
- LinkedIn
- WordPress
- DreamHost
- Dashlane (password manager)
- LastPass (password manager)

For a more complete list of sites offering two-factor authentication, visit: **https://twofactorauth.org/**.

ACTION PLAN

1. Audit passwords.
2. Enable Two-Factor Authentication wherever possible.
3. Deploy a password manager.
4. Configure the password manager to generate 16+ character passwords for each accessed site using upper/lower case letters, numbers and special character.
5. Protect your password manager with a strong, passphrase-based password (16+ characters). Use Two-Factor Authorization to secure your password manager.

brandprotect™

www.brandprotect.com
sales@brandprotect.com |

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect, helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.