US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Password Security, Protection, and Management

Alexa Huth, Michael Orlando, and Linda Pesante

Every Password Is Important

With the many ways we use the Internet, it's easy to consider some passwords less important than others. However, all passwords are important because wrongdoers can piece together the information you store online and use it for their benefit. They can even use information you share on social media networks. And commercial websites give customers the ability to store billing and shipping addresses along with credit card information. This paper offers recommendations for protecting your information by selecting strong passwords and storing and managing them safely.

Creating and Protecting Your Passwords

The complex methods that attackers can use to gain access to your personal information are becoming more easily accessible to wrongdoers and are increasingly effective. It is important to avoid the common mistakes that give these individuals the opportunity to exploit your personal data.

Common Mistakes and Remedies

Mistake #1: Using a weak password. Selecting a weak password is like closing your front door but not locking it. A password is weak if it can be guessed easily. Examples of weak passwords are dictionary terms, common phrases, your name or birthday, or "password" and " p@ssw0rd".

Remedy: The easiest way to create a secure password is to use a pass*phrase*. A good example comes from the Microsoft Safety & Security Center (italics added):

> Start with a sentence or two. *Complex passwords are safer*.
> Remove the spaces between the words in the sentence.
> *Complexpasswordsaresafer*. Turn words into shorthand or intentionally misspell a word. *ComplekspasswordsRsafer*. Add length with numbers.
> Put numbers that are meaningful to you after the sentence.
> *ComplekspasswordsRsafer2011*.

The Microsoft exercise shows how you can create a passphrase that is both strong and easy to remember. It follows several safe password guidelines: it is long, it is not a common phrase, it includes numbers, and it includes both lowercase and uppercase letters. The one guideline missed in the example is to use special characters such as punctuation or, for example, a dollar or pound sign.

Mistake #2: Using the same password for every account. This is a security concern because if an attacker guesses or cracks a password for one account, he or she can access all your accounts. Even if the attacker gets the password for a relatively nonsensitive account; he or she can reuse it on sites where, for example, billing, payment, health, and other private information is stored. Using the same pattern for your passwords is also risky. By learning your current password structure, attackers can increase their chances of guessing passwords for critical websites such as your bank account or your company's email account.

Remedy: Use a different password for each website you access. A password manager—essentially an encrypted database— can help you store all these unique passwords and passphrases in one safe, well-protected place. (See the next section for details about password managers.)

Mistake #3: Exposing passwords to others. This can mean logging in from a public computer, keeping a note with passwords written on it where it can be found, or sharing your passwords with others. It can also mean having your web browser store your password information. If you get a prompt asking if you want a site to remember your password, say "no." The reason is that most browsers store passwords encoded in a way that is publicly known, and thus easy to decode. Password recovery tools, which are easily available online, enable anyone to see all the passwords stored in the browser and open users' profiles.

Remedy: Avoid public computers and public access networks. If you happen to use one, do not access private, sensitive, or business information; and change your password afterward. In all cases, keep your passwords well protected, perhaps by keeping them in a lockbox or safe, or in an encrypted file or password manager. Avoid sharing passwords. Occasionally, you might have a guest who needs access to your home wireless network. Share your *strong* passphrase only with a visitor you trust, or type it in yourself. (It's common courtesy as well as a good security practice to look away when someone is typing his or her password.)

Password Managers

A password manager is software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master passphrase. It is one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts—without writing them down on a piece of paper and risking that others will see them. When using a password manager, you have one master passphrase that protects all of your other passwords. This leaves you with the ease of having to remember only one.

Types of Password Managers

As Neil Randall pointed out in *PC Magazine* over a decade ago, "Password management utilities have proliferated with the growth of the Internet and, as Web users log on to more and more password-protected sites, have become almost indispensable tools."

There are many types of password managers. A *desktop* password manager is software you install on your computer's hard drive; it stores your user name and password only on that computer. You can use a *portable* password manager on your smart phone and other portable devices. Or you may choose to store your passwords on the *website* of a password management provider or choose *multi-factor authentication*, where you use a combination of ways to access a password manager on your desktop; for example, a smartcard or USB drive plus a password or, perhaps, a fingerprint. Some password managers can *create new passwords for you.* This eliminates the need for you to come up with dozens of unique and complex passwords and passphrases.

In *PC World*, Paul Mitchell describes a new type of password manager that eliminates the worry about where your password manager is located: "The makers of an emerging breed of password managers are striving to provide secure online access to your passwords in the cloud and give you a synchronized, local copy of your password database on every computer and mobile device, no matter what operating systems, browsers or mobile platforms you use." If all the information is stored in the cloud, you can access it from any of your devices at any time. Moreover, in effect, the cloud provider creates a backup of your password manager file. If you do not regularly back up your desktop files, a cloud-based password manager may have important features for you to consider.

Choosing a Password Manager

Consider the type of password manager that best suits how and where you work. This is where research into the type of password manager is necessary. Ask yourself what type of passwords you will be storing and where you will most often access these sites. For example, if you have passwords only for sites that you access at home, you would not need the password manager to be stored on your mobile device. If you store a password manager on one computer and need to access your passwords on another computer, you run into problems. On the other hand, if you are using only one computer, the storage decision becomes easier. If you use a generator of one-time passwords for all your accounts, you do not have a set of passwords to store—though you may have a set of usernames.[1] You need to consider whether acquiring a password manager is the best way to handle your usernames. If you have a mix of passwords you choose and one-time passwords that are generated for you, a password manager can be useful for the passwords you choose.

[11] Note that you still need to protect your one-time password during the time it is valid, not writing it down or letting another person—a potential attacker—see it.

After you know your needs, you can investigate particular products.

When researching the products, determine the security measures of each. Does the password manager use strong encryption? Does it have a lockout feature? Does it include protection from malicious activity, such as keystroke logging—and which kinds of activity?

Evaluate ease of use and convenience. Look at the functionality and the interface features and think about how you will like them over the long term. Also examine support from the vendor/provider. Look for (and evaluate) online documentation, and find out how the company interacts with its customers: email? telephone? chat? other ways?

Consider cost. Is there a one-time cost or a recurring fee? Some password manager vendors provide a free trial period or charge for certain features. If the latter, which features do you consider worth the cost?

Supplement your own evaluation by searching the web for articles on the top-rated password manager and analyses of the strengths and weaknesses of various products

Finally keep risks in mind. Note particularly that there is both convenience and risk associated with storing your passwords in the cloud, as noted in a previous US-CERT paper[2] and there is the potential for attacks on cloud password managers. In May 2011, Brennan Slattery, reported in a *PC World* that the provider of an online password manager identified unusual network traffic of a size that could indicate an email address and password compromise. All customers were asked to change their master password.

Remember also that there is a risk with using your password manager in public locations, specifically if you leave the password manager open in the background on the computer. Also if you open your password manager on a public computer you may be taking the risk of key logging software being installed on the computer. This software can capture the information that you type on the keyboard, and a malicious user could steal your master password.

In all cases, you must protect your master password well; it's best to memorize it rather than write it down.

Some Final Words on Password Managers

With the growing number of necessary passwords and the amount of information that people have stored in online accounts, the Internet is an attractive place for malicious users to steal your personal information. By using complex passwords and passphrases and choosing a password manager that fits your password use habits, you can keep your information secure and protect yourself from identity thieves.

Before you decide on a password manager, read reviews of the various products in order to understand how they work and what they are capable of doing. Some reviews include both strengths and weakness. Also do your own analysis by reading background information on

[2] "The Basics of Cloud Computing," by A. Huth and J. Cebula.

vendors' websites. When you have chosen a password manager, get it directly from the vendor and verify that the installer is not installing a maliciously modified version by checking an MD5 hash of the installer[3]; if a hash is not available, request one from the vendor; if the vendor cannot provide a verification method, be skeptical. Although moving to a password manager may take a little effort, in the long run it is a safe and convenient method of keeping track of your passwords and guarding your online information.

Further Reading

1. Huth, Alexa and Cebula, James. "The Basics of Cloud Computing." 2011. Available from: http://www.us-cert.gov/reading_room/USCERT-CloudComputingHuthCebula.pdf (accessed March 1, 2012).

2. McDowell, Mindi et al. "Choosing and Protecting Passwords," US-CERT Cyber Security Tip ST04-002, 2009. Available from: http://www.us-cert.gov/cas/tips/ST04-002.html (accessed March 1,2012).

3. Microsoft Safety & Security Center. *Create Strong Passwords.* 2012. Available from: http://www.microsoft.com/security/online-privacy/passwords-create.aspx (accessed March 1, 2012).

4. Mitchell, Robert L. "Best Password Managers: Top 4 Reviewed," *PC World,* 2010.Available from: www.pcworld.com/article/208113/best_password_managers_top_4_reviewed.html (accessed March 1, 2012).

5. Randall, Neil. "Manage Your Passwords," *PC Magazine*, 2000. Available from: http://www.pcmag.com/article2/0,2817,31115,00.asp (accessed March 1, 2012).

6. Rubenking, Neil J. "Six Great Password Managers," *PC Magazine,* 2011. Available from: http://www.pcmag.com/article2/0,2817,2381432,00.asp (accessed March 1, 2012),

7. Slattery, Brennon. "LastPass, Online Password Manager, May Have Been Hacked," *PC World*, 2011. Available from: http://www.pcworld.com/article/227223/lastpass_online_password_manager_may_have_been_hacked.html (accessed March 1, 2012).

[3] If you are not familiar with this verification method, the website http://www.openoffice.org/dev_docs/using_md5sums.html describes several methods, including ones for various operating systems. You can also search for products and their instructions, including browser plug-ins.