This is the second of a series of documents created by St. Andrew's parishioner Kelly Bourne, a retired computer security professional.

CyberSecurity Article #2 - Passwords

Many experts have predicted its demise, but passwords remain the most common method of authentication for accounts, applications and websites. Virtually everyone that uses a computer has had to use or create a password.

Because they're so widely used, cybercriminals try to determine the passwords of potential victims. If they're able to log into your account(s) using an uncovered password these criminals can hurt you in many ways, including:

- Steal funds from online sources like bank accounts or retirement accounts.
- Learn personal information about you that can lead to identity theft.
- Open new loans or credit card accounts under your name.
- Obtain health care treatment using your identity.
- Damage your reputation by sending out spam from your email account.
- Make online purchases using your credit card accounts.

There are several methods of discovering or 'cracking' passwords. Some of the most common are:

- Phishing is sending emails to a potential victim under false pretenses. The bogus email tries to convince the recipient to open an attachment or click on a link in the email. If the victim falls for the deception, then malware (malicious software) will be installed on his or her computer. This malware can steal personal information including passwords.

- Social engineering is when a bad guy tricks potential victims into revealing personal information including passwords. Social engineering attacks can be via email, text messages, phone calls or in person.

- A keylogger is a piece of software installed on a victim's computer that records every keystroke made on the device. All the victim's keyboard activity, including account IDs and passwords, get sent to the criminal. Keyloggers can be installed by phishing emails, social engineering or by visiting an infected website.

- Brute force attacks are when a hacker enters every possible password into an account looking for the correct one. Tools called password crackers are used during these attacks. The shorter and simpler a password is, the more likely it is that a brute force attack will uncover it.

- Credential stuffing attacks occur when lists of legitimate credentials, i.e. account IDs and passwords, exposed by previous data breaches are used to gain access to other accounts. If your credentials were revealed by a data breach and the same passwords was used for multiple accounts, your other accounts may be compromised.

The average user has a surprisingly large number of passwords. NordPass, a computer security firm, reports that users typically have 168 passwords for personal use and 87 for business-related ones. Dashlane, a password manager vendor, estimates the average user has 240 accounts needing passwords.

The human brain isn't capable of remembering 200+ different passwords. Studies show that the average person can reliably remember between four and seven passwords. How do users get around this difference?

One common way users deal with numerous passwords is by reusing the same password for multiple accounts. Reusing passwords is extremely risky. The danger is that if a hacker uncovers or "cracks" it then he can access all of the users' accounts using that password.

Using simple passwords, e.g. 'abcdef", 'password' or '123456' is another risk. Hackers have lists of simple passwords that they tried when cracking into accounts. Every year lists of the most frequently used passwords are published. An Internet search of "most often used passwords" will display them. If any of your passwords are on these lists, change them immediately!

Never changing passwords is a choice some users make. The risk is that if a password is never changed hackers have unlimited time to guess it. Once they've cracked or discovered it, they can access that account indefinitely.

Choosing a new password that is a simple variation of the current passwords is a bad idea. For example, if the existing password is "secret" don't replace it with 'secret1.' Software cracking tools try variations like this.

Writing down all of your passwords in a computer file or on a piece of paper is a common practice. It's true that this can help record numerous passwords, but it involves some risk. If someone else sees that file or piece of paper, then all of the accounts are at risk.

Some steps that can be taken to protect your accounts are:

Choose strong passwords, i.e. ones that have the following characteristics:

- Passwords should be a minimum of 12 to 14 characters long. Short passwords can be easily guessed or discovered by cracking tools.
- Passwords should include upper- and lower-case letters, numbers and special characters like #, @ or &. This combination makes it almost impossible to guess a password. It also makes cracking it significantly more difficult.
- Passwords shouldn't be based on your name, birthdate, address, favorite sports teams, pet names, etc. Hackers can find an amazing amount of personal information like this on the Internet, particularly on social media sites.
- Passwords shouldn't be words found in dictionaries. Password cracking tools often use all dictionary words when trying to break into accounts.
- Passwords written on a Post-It® note and attached to the monitor or under the keyboard aren't secure.
- Every account should have a unique password. Reusing passwords for multiple accounts is extremely dangerous.
- Passwords should be updated regularly. Experts recommend changing passwords every 60 to 90 days.

Using a passphrase instead of a password is one way to keep an account secure. A passphrase is a string of words that is easily remembered but would be hard to guess or crack. Some examples of passphrases are:

- TheSoundOfMusicIsMyFavoriteMovie
- InColdBloodByCapote
- DoYouKnowTheWayToSanJose

Passphrases can be made more complex by substituting numbers for letters, capitalization or adding underscore characters. These passphrases are variations of the previous examples.

- TheS0undOfMusic1sMyFav0riteM0vie
- INC0ldBl00d_ByCapot3

Using a password manager is another way to safeguard your accounts. A password manager is like a vault that stores all your passwords. You just need to remember the password to the password manager, and it can unlock all your accounts. I'll describe how password managers work in a future article.

-Kelly Bourne