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

Cyber-safety Article #5 - Protect Your Passwords

Criminals from around the world want to steal passwords for your online accounts. Examples include email accounts, bank accounts, Facebook accounts, eBay accounts, and Amazon accounts. They have many ways of getting passwords, but you can take steps to help protect your passwords.

Knowing your password lets criminals log into and take over the account. If a hacker is able to log into your account, he can change the password and lock you out. Having control of your account enables them to steal from you. Cybercriminals are able to steal assets from bank accounts, retirement accounts and even frequent flyer accounts. They're even looking to steal digital assets from victim's online game accounts.

If you have accounts with online retail stores, a hacker can make purchases and have the purchases sent to an address where he can safely pick them up. He'll get the merchandise and stick you with the payments.

Controlling your email or social media account is also valuable to a criminal. A hacker can use your account to communicate with your contacts and scam them. They can glean through your old emails looking for personal information like credit card numbers, passwords, and financial details that can be exploited.

If a hacker can accumulate enough personal data about you from the accounts he can access, then he can commit identity theft. He will apply for new credit cards, take out loans and open accounts with online merchants in your name. He'll max out those accounts and you may be stuck paying for it.

Some criminals don't steal from you directly. They choose to sell your account IDs and passwords on the Dark Web. Oher criminals will purchase your credentials and steal from you.

Methods to Steal Your Passwords

There are many methods that criminals use to steal passwords. In a phishing attack scammers send emails to potential victims that appear to be from legitimate sources like a bank, clergy members, friends, Amazon, eBay or a government agency. The email may claim that your account has been compromised or locked. To correct the problem, you're instructed to click on a link in the email and log into the account. The link leads to a website that looks legitimate but is controlled by criminals. If you log into it, they'll capture your ID and password. Never trust a link included in an email! Always enter the site's URL into a browser yourself or use the "Favorites" feature of the browser to get to authentic websites.

Social engineering attacks are another way to trick victims. The scammer may call, text or email you pretending to be a technician from Microsoft, customer support from Facebook, a law enforcement officer or a bank official. They'll have a convincing story explaining why you should reveal your account ID and password. The story may be that they need this information to protect your account, correct a problem with your computer, or to catch bad guys. Don't believe them! No legitimate business will ever ask you to reveal your password.

Another way criminals get victims' passwords is to infect a file with malware and attach it to email. The email will try to convince recipients that they need to open the attachment. If you open it, malware will be installed

on your computer or phone. The malware might be a virus, ransomware or a keystroke logger. Whatever type of malware it is, its goal will be to steal your assets or personal information. This type of attack can be prevented by never opening an attachment unless you confirm with the sender that it is legitimate.

What to do if your password is stolen

If you're the victim of a password scam, change all affected passwords immediately! This might involve multiple accounts. When creating a new password make sure to pick a strong one and never use the same password for multiple accounts. New passwords shouldn't be a variation of the old password, for example by adding a "1" to the end of it.

How can you determine if your password has been stolen?

- The password that should allow you to log into an account isn't working.
- You receive notifications that the account was logged into, and it wasn't you.
- You receive a data breach notification letter from one of your account vendors that your credentials have been exposed.
- Security tools like HaveIBeenPwned or The Stolen Password Scanner can indicate that your password has been found on the Dark Web. Some password managers will also notify you if your account credentials have been compromised in a data breach.

Tips to prevent having your password stolen

- Have strong, unique passwords for every account. If the same password is used for multiple accounts, then if a criminal is able to access one account, he gains access to all of them.
- Never click on links in unknown emails! Criminals frequently send out emails or texts telling victims that their account has been compromised or locked. If you hover over a link, you can see the actual web address it will take you to. Scammers frequently create an address that differs from the real one by only a letter or two.
- Legitimate companies and government agencies will never call you unexpectedly. Don't trust anyone if you didn't initiate contact with them.
- Emails or texts that pressure you into acting immediately are always scams.
- Set up multi-factor authentication (MFA). It can protect your account even if a criminal has the password.
- Limit the personal details you post on social media. These details can be clues to your password. Personal information can be used to help social engineers convince you that they have similar interests or that they're someone you can trust. For example, if you have many posts about golfing, they might send you an email with an attachment that promises free or discounted rounds of golf. The attachment really contains malware.
- Never share your passwords with anyone. No legitimate company representative will ever ask you for your password.
- Never allow anyone to remotely control your computer. Allowing this will let them steal from you.

- Using a password manager allows you to have unique, strong passwords for all your accounts.
- Never believe or trust any communication that you didn't initiate.

It's a sad reality but we live in a world where it isn't safe to trust strangers. If you're contacted by someone you don't know personally there is a significant chance it's a scam. If your gut tells you that something is wrong, then trust your instincts and hang up or ignore the text or email. The old saying "better safe than sorry" has never been more applicable than today.

- Kelly Bourne