WILLOW CREEK WEALTH MANAGEMENT

Cybersecurity Guide

Rev. 1/2025

Table of Contents

1. Background.......3

2. Phishing.......3

2.1. What is Phishing?.......3

2.2. Guarding Against Phishing.......3

3. QR Codes.......4

4. Identity Theft.......4

5. Devices.......5

5.1. Public Wifi.......5

5.2. VPN (Virtual Private Network).......5

5.3. Firewalls.......5

5.4. Mobile Device Security.......5

5.5. Stolen Device Protection.......5

5.6. Device Encryption.......5

5.7. USB Drives.......6

5.8. System Updates.......6

5.9. Backups.......6

6. Credentials.......6

6.1. Strong Passwords.......6

6.2. Multi-Factor Authentication (MFA).......7

6.3. Password Managers.......7

6.4. Passkeys.......7

7. Want to Learn More?.......7

1. Background

Let's start by taking a 30,000 foot view of the cybersecurity landscape and see what areas are most concerning to us and how the landscape as changed in recent years:

- Cybersecurity threats continue to evolve and it is therefore important to remain vigilant and up-to-date in order to protect yourself.

- Over the last five to ten years, the most significant threat to individuals has become phishing, typically through email but also through text messages, QR codes, phone calls, etc.

- The corporate world has seen a rise of both phishing and ransomware (which is malware that seeks to encrypt sensitive data and hold it hostage, demanding a ransom be paid before the data is released back to the organization). Ransomware is a threat to individuals, but it is typically a minor one.

- Identity theft continues to be a concern and it is hard to prevent, but there are steps that can be taken to remain vigilant.

- Strong passwords continue to be extremely important and most common breaches are due to weak password or not using multifactor authentication.

- The risks of cybersecurity breaches cannot be eliminated, but they can be mitigated to a large degree through various safeguards and best practices that are outlined below.

2. Phishing

2.1. What is Phishing?

Phishing is by far the most common attack vector associated with individuals and it has become an exponentially growing concern for corporations. Computer systems and hardware have become very good at preventing intrusions, which is why most attacks have moved toward attacking the human element through social engineering and other schemes. This is why phishing is so prevalent—it circumvents the software and hardware protections *and it works*.

The goal of phishing is to steal your login credentials (username and password) to services that you use and then exploit the data that can be accessed. The attacker essentially attempts to trick you into just giving them the credentials.

2.2. Guarding Against Phishing

We recommend a four-step process to scrutinize emails to ensure legitimacy:

- ✓ **"The Smell Test"** – Does it make sense for me to be receiving this email? Do I get email from this sender regularly? Is it asking me to take action on something that I was not expecting ahead of time? Think about things such as DocuSign signature requests or password reset emails. 99% of the time, you are expecting these emails. Unsolicited emails asking you take action are suspicious.

- ✓ **Who is actually sending this?** Take the time to review the sender's email address and, in particular, the domain name that is originating the email. If it's coming from a free email account, such as Hotmail, Yahoo, Gmail, etc., but purporting to be from a legitimate source, that's a very good indicator that something is awry.

- ✓ **Are there attachments?** Attachments to emails—especially if you were not expecting them—are highly suspicious and should be treated as such. These are common vectors for viruses and malware and can also be used in phishing attacks. Do not open attachments from sources that you do not fully trust or were not expecting.

- ✓ **Scrutinize the links.** The links in an email are usually what will get you. They will aim to send you to a website that looks real but may not be. The goal here is for the attacker to steal login credentials by tricking you into just simply giving them away. Hover your mouse cursor on links in emails and look at the domain name (i.e. "docusign.net") for anything that does not look legitimate. Often, we see these pointing to gibberish domains or domains in foreign countries (i.e. ".ru" which is Russia). Just because a web address is long does not mean anything—it's important to look at the domain itself.

The key here is that you need to do *all four of these checks* as sophisticated attackers can manipulate some of these items.

3. QR Codes

QR codes are becoming a common vector for phishing attacks, which aim to get you to scan a code that takes you to a website which attempts to steal your login information. Often these masquerade as needing to "verify your identity" through an email account or other common login. Be very careful about QR codes and only scan them from sources you trust (and definitely do not provide any login credentials to a prompt from a QR code).

4. Identity Theft

Identity theft is challenging to entirely prevent, but good financial hygiene includes keeping a close eye on credit cards and your credit reports. Many credit card companies now offer free credit reports that flag activity. One step further are services like LifeLock which offer monitoring of credit for a monthly fee. The strongest step is a credit freeze at the main credit reporting agencies, but keep in mind that such a freeze also needs to be removed before applying for any sort of credit in the future. This is not usually recommended unless you have been a victim of fraud in the past.

We do recommend that you opt-in for electronic delivery of all sensitive documents from Willow Creek, your custodians, and your other financial institutions. Mail theft is a common approach for identity thieves to obtain your information, so minimizing sensitive information traversing the mail is a good step.

5. Devices

5.1. Public Wifi

Public wifi should be treated with caution as it opens your data communications with the Internet and potentially your device to more direct intrusion opportunities for those with ill intent. When possible, use cellular rather than public wifi—it is an isolated and encrypted connection. If you need to use public wifi, make sure you are doing benign things, such as reading the news and checking your email. Steer clear of transacting any sensitive data if possible.

5.2. VPN (Virtual Private Network)

A VPN is a service that you subscribe to which, when enabled, fully encrypts that data you send to/from your device out to the Internet. A VPN is recommended if you commonly use public wifi and are using those networks for sensitive tasks, such as for business. If you do not fall into those categories, a VPN is generally not necessary and the approach outlined above using a cellular connection is often the simplest and lowest cost approach.

5.3. Firewalls

Laptops and mobile devices have software firewalls that make it more difficult for someone to directly attack those devices when on other shared networks, such as public wifi. Most cell phones and tablets have a firewall enabled by default that you cannot turn off. Laptops are a different story—be sure to review your MacOS or Windows settings to ensure your firewall is enabled if you travel with your device or use public wifi.

5.4. Mobile Device Security

For phones and tablets, it is recommended to always use at least a six-digit passcode (not the four-digit option) and to enable biometrics (facial recognition or thumb print). Be sure that your passcode is not easily guessed or just a sequence of the same number six times.

5.5. Stolen Device Protection

Apple phones have a feature called Stolen Device Protection that is disabled by default and we recommend enabling this. This feature makes it more difficult for someone to steal your phone, wipe your data, and re-sell the device as it puts in place a timeout based on location to perform those tasks and also requires other identification factors to do so.

5.6. Device Encryption

We recommend that any device that leaves the home have an encrypted drive. Most mobile devices, such as phones and tablets, are encrypted by default and you cannot disable it. Whereas laptops are almost never encrypted by default. If you travel with a laptop, look in to enabling drive encryption as this makes your data useless and inaccessible by force to someone that may steal your device.

For MacOS, the encryption system is called FileVault. For Windows, it is called BitLocker. Each has a separate process for enabling this feature.

5.7. USB Drives

USB drives are commonly used to plant viruses and malware than can infect your computer. Never connect a USB drive to your computer that you do not fully trust. If you bought it on Amazon and use it for backups—great! If you found it sitting around an airport or someone handed it to you—definitely not.

5.8. System Updates

Updates to your operating system on your laptops, desktops, phones, and tablets bring security enhancements almost weekly. Be sure to keep up with your system updates so that you have the latest protection against new exploits.

5.9. Backups

Backups are incredibly important in safeguarding against accidental deletion, stolen devices, or hard drive failures—all of which happen often. A good backup routine is essential and there are many different approaches to this depending on the sensitivity of your data, the frequency of new data being created, and the hardware you are using. MacOS has a feature called Time Machine that works very well with an external USB hard drive to take incremental backups of your data. Windows also has backup tools that work similarly. Some choose to make manual backups of files.

The best backup strategies are called a 3-2-1 approach:

- ✓ **Three** copies of your data.
- ✓ **Two** different types of media (external drive, cloud, etc.).
- ✓ **One** copy offsite.

Remember that backups are about mitigating potential data loss, so the more copies the better and it’s best to have copies in different places to protect against loss from disasters.

We are happy to discuss the pros and cons of different approaches and help find a solution that meets your needs.

6. Credentials

6.1. Strong Passwords

The most important part of protecting yourself is to utilize strong password methods. A strong password meets the following criteria:

- ✓ **Complex**: includes uppercase, lowercase, numbers, and special characters.

- ✓ **Long**: the length of a password is the most important factor in strength; an 8 character complex password can be broken in a couple of minutes by brute force attack (guessing it with a computer), whereas an 18 character complex password would take 26 trillion years (with current computer power). The current standard is at least 12 characters, but we recommend more for things like password managers (20+).

- ✓ **Unique**: you should never reuse the same password twice… anywhere.
- ✓ **Rotated**: passwords for highly sensitive things (your password manager, financial institutions, health websites, etc.) should be rotated once or twice per year.

6.2. Multi-Factor Authentication (MFA)

Strong passwords are great, but even they pose risks when password databases are stolen or circumvented. Multifactor Authentication (MFA) – often implemented with a code sent to your phone via text message – is a gamechanger and largely prevents intrusions when enabled, even if the attacker has your password. MFA is not foolproof and MFA codes can be phished from you, but it is highly recommended that you utilize MFA everywhere it is available.

6.3. Password Managers

How does one safely retain all these long, complex, and unique passwords? That is where password managers come in. There are many good ones out there, such as LastPass, 1Password, Google's built-in manager, and Apple's built-in manager (formerly Keychain). The important part is that you use one for everything. We are happy to discuss the pros and cons of different options with you.

6.4. Passkeys

The future of passwords is no passwords! That's the idea behind passkeys, which started rolling out widely on websites in early 2024. These are essentially a unique key pair that a website can match up with the half that is on your authorized device and allow you to sign in securely to a service without entering a password. The ability to do this depends on the use of biometric authentication on the device using the passkey. This is a more convenient and more secure way to log in to a service than by entering a password and using MFA. We encourage you to give it a try as it is the direction that passwords are going.

7. Want to Learn More?

Sign up for a complimentary Cybersecurity Checkup. Details and sign-up links are available here: https://willowcreekwealth.com/cybersecurity-checkup-program/