Effective Data Security for the Wealthy

In the constantly evolving world of technology, cyber criminals are finding more unique ways to steal your personal information. Since the beginning of the COVID-19 pandemic, the FBI has reported a **300 percent increase in reported cybercrimes.** Wealthy individuals are often a prime target for the unscrupulous. While data security is a constant uphill battle, there are five simple steps you can take to keep your personal information safe.

1. **Avoid Sharing Personal Data**

   In your daily life, avoid sharing identifiable information such as your social security and credit card numbers. Cyber criminals will try to obtain this information from you via false-legitimate email addresses and phone numbers. It is especially important to:

   - determine the legitimacy of anyone attempting to contact you over the internet or via your phone.
   - be aware of the common cyber-criminal practice of phishing. Phishing occurs when cyber criminals pretend to be a contact from a reputable source to obtain your personal data. According to a Verizon study, 94 percent of cyber-attacks originate from phishing.
   - never give any identifiable information to an unidentifiable source.
   - always verify the legitimacy of an unfamiliar person who emails or calls you by consulting with your partners.
   - block the email address or phone number if not legitimate.
   - ensure none of your information has been compromised. If it has, notify the authorities.

2. **Use Strong Passwords**

   Computing has advanced to extremely advanced levels in the short amount of time that the technology has been available to the public. Cyber criminals have access to computers that can decipher a weak password in less than a day. Yet, a strong and unique password can take years for even the most powerful computers to decipher.

While it may seem drastic to change your easy-to-remember password, the only difference between a strong and weak password is about six characters, which always includes numbers and a special character. For example:

> You use the same seven-character password, walnuts, across multiple websites. If any of the website's encryption keys were leaked, this password could be deciphered in approximately three seconds. If you were to change this password to Walnuts17!, it would take decades to be cracked by even the most advanced technology.
>
> Always include at least one capital letter, one number, and a special character in your password. The standard length for a strong password is 9-15 characters. If you have trouble remembering your passwords across multiple sites, consider utilizing a password manager. This will automatically create and store passwords for any accounts you create on the web.

3. **Connect to secure Wi-Fi**

In an office or home setting, the Wi-Fi network should always be hidden so only authorized users have access to the network. In public, many cyber criminals will sit and wait on open Wi-Fi networks for users to reveal their information:

- never use public Wi-Fi networks when dealing with personal information, as you are at the mercy of any cyber-criminal who might be taking advantage of the unsecure network.
- if you cannot connect to a secure Wi-Fi network, consider using a Virtual Private Network (VPN). A VPN is essential when working outside of your office or on a trip.
- VPNs can create a private network specially for you so that if you connect to public Wi-Fi, you still have a layer of protection between you and cyber criminals.

Many companies provide VPNs for their employees, and some are safer than others. If your company does offer a VPN, make sure you know how to connect and use it. If you are planning on using your own VPN, be sure to do some research as there are many excellent VPN options available to you.

4. **Enable firewall protection**

The first line of defense against cyber criminals comes before your password, VPN, or your Wi-Fi network. Firewalls filter out unauthorized users by monitoring your network traffic and setting filters to only let safe traffic reach your network. Firewalls have become a standard practice for any business that will be accessing the web. All Windows and MAC operating

systems include a basic firewall. Even this included version can make the difference between you being an easy target or protected against cyber criminals.

5. **Invest in security systems, keep your software updated**

   It is standard practice for any piece of technology involving online transactions to have security software. Because cyber criminals are often after money, devices with financial information moving across their networks are prime targets.

   - Use antivirus software and back up your files which can make the difference between protecting your data and losing everything in the event of a data breach.
   - Install computer updates as soon as they occur. These updates are often rolled out to patch holes in the security of your device. Older versions of installed software are unsecure to have on your device.

Data Security for the Wealthy: What *NOT* to do

- Don't share personal data with unverified contacts.
- Don't post any private or sensitive information on public sites.
- Don't interact with links, QR codes, or messages from unknown sources.
- Don't use weak passwords for your accounts.
- Don't share your passwords with anyone.
- Don't connect to unsecure Wi-Fi (coffee shops, libraries) when working with sensitive documents.
- Don't leave your device vulnerable; use a firewall.
- Don't neglect the need for security software (antivirus, data backups) on your device.