GARDECAPITAL

July 2024

Cyber Health Series

Information Security and Your Protection

The importance of protecting your personal information cannot be overstated in today's interconnected world. Personal information, such as social security numbers, credit card details, and login credentials, is highly valuable to cybercriminals. When such data falls into the wrong hands, it can lead to identity theft, financial loss, and severe privacy violations. The consequences can be devastating for individuals, including damaged credit scores, drained bank accounts, and long-lasting emotional distress. Thus, safeguarding personal information is critical not just for personal security but also for maintaining trust in digital transactions and communications.

At Garde Capital, we have a fiduciary responsibility to help in any way we can with the protection of your data. That means selecting custodians for our clients such as Charles Schwab Institutional and Fidelity that have the highest levels of security and ensuring that only you or those who you have given specific authorization can access that data and act on your behalf. It also means doing everything in our power to create processes that improve the odds of your data remaining secure over time.

Common Fraud Techniques

Fraudsters employ various techniques to gain access to personal data, often exploiting human error or technical vulnerabilities. Some of the most common methods include:

- **Phishing:** Phishing involves sending deceptive emails or messages that appear to be from legitimate sources, such as banks, government agencies, or well-known companies. These messages often contain links to fake websites designed to steal login credentials, personal information, or financial details. Variants of phishing, such as spear phishing (targeted at specific individuals) and smishing (phishing via SMS), are also prevalent.
- **Malware:** Malware, or malicious software, includes viruses, trojans, ransomware, and spyware. These programs can be installed on a user's device without their knowledge, often through infected email attachments, malicious websites, or software downloads. Once installed, malware can steal personal information, monitor online activity, or even lock users out of their devices until a ransom is paid.
- **Data Breaches:** Data breaches occur when hackers gain unauthorized access to large databases of personal information maintained by companies, government agencies, or other organizations.

These breaches can result from vulnerabilities in software, weak passwords, or insider threats. The stolen data is often sold on the dark web or used directly by criminals to commit fraud and identity theft. An article by USA Today covers an incident in which a file with nearly 10 billion passwords were posted to a hacking site. With these breaches becoming more and more common, it is now more important than ever to be mindful of updating and safeguarding your personal information.

What You Can Do

Over the many years we have been working with clients, we have watched the techniques used by fraudsters become more elaborate and harder to catch. Still, there are some simple things that we can do to avoid some of the catastrophic consequences of cybercrime.

You may not know it, but email may be the #1 gateway to cybercrime. Your email contains a host of information that a fraudster can use. We often send our own personal data over email in an unencrypted format. It is very easy for someone to hack into your email and read your messages. A fraudster can even send emails to others making it look like you are the one communicating.

Here are some general tips and habits to adopt when it comes to email and other forms of electronic communication that will help protect your personal information:

- **Email Encryption**: When using email, try to avoid sending any of your personal data such as credentials, credit card numbers, account numbers, social security numbers any other item that can help someone gain access to your accounts. If you need to send your data, ask the recipient to provide a secure upload link that will encrypt the information and send directly to them.
- **Reason Before You React - be skeptical of any unsolicited communications via email, texts, or calls**: These days, we are likely to get countless emails, calls and texts that look familiar from trusted sources that we think we know. They may ask us to click on something like a DocuSign link or a gateway to a site to enter credentials. You may even get a text message from what looks to be your bank that says suspicious activity has been detected in your account and will want you to click a link to verify your identity. While you do want to respond quickly to possible threats, you will need to take some time to consider if the message is legitimate. If you see anything that looks out of the ordinary, *do NOT click on any links or respond directly to the message.* If you have a question about whether it is legitimate, call the sender or company in question using a phone number known to you, not the number that appeared in the email or text message.
  If you receive an unsolicited call, do not share any information with anyone calling you from a bank or other financial institution, even those that you trust. If you receive unsolicited calls of this nature and you wish to investigate whether they are legitimate, simply hang up and call your institution back at a number known to you in advance.

- **Password Updates and Increase Password Complexity:** Update your passwords on a regular basis. Use strong and unique passwords. Password manager tools such as LastPass, 1Password, or Dashlane can help you create and manage strong, unique passwords.
- **Multi-factor Authentication:** Apply two-factor authentication to any site that contains your sensitive data. This could be a code that is sent via text, phone call, email or generated from an authentication application.
- **Digital Housekeeping:** Routinely remove files with sensitive information from your hard drive and make sure they are stored in a secure location with two-factor authentication. Malware can be used by fraudsters to gain access to your machine without you knowing it, and once there, they will have instant visibility of this information. Additionally, keep systems and software up to date and install a strong, reputable anti-virus program.
- **Cryptocurrency Scams:** If anyone suggests that you send them funds using Bitcoin or other crypto currency, this is almost certainly fraud.

These are just some of the many tips that can be used to maintain good cyber heath. Check out these and other ideas from cisa.gov.

What if Fraud Occurs?

These are some helpful strategies for reducing or eliminating the possibility of fraud with our accounts and data. However, even the most sophisticated strategies may not protect us completely. Millions of people each year become victims of this type of fraud. If you feel that your financial situation has been compromised in any way and you would like some ideas on how to manage the impact, please see our January 2023 newsletter: Fraud and Identity Theft for some steps that may help.

Cybersecurity and the protection of your personal information will be an ongoing effort for all of us and promises to get only more challenging as time goes on. At Garde Capital, we are committed to your safety and security, and we will keep you up to date on enhancements to our processes as those occur. In the meantime, if we can be helpful with any aspect of the protection of your assets or information, please do not hesitate to let us know.

Please find this newsletter and others on our website at http://www.gardecapital.com.

This article was published by Garde Capital, Inc. a Seattle based Registered Investment Advisor that provides wealth management solutions to individuals and families, nonprofit organizations, and corporate retirement plans.