DIGITAL
**PRIVACY &
PROTECTION**

A Guide for Business Owners

Protecting You & Your
Family from Cyber Threats

June 2023

www.dpripro.com/businessowners

Business owners are compelling targets for cybercriminals. They recognize that business owners work constantly including at night and on weekends, at home and on vacation. Additionally, being unable to operate the business even for brief periods of time has an enormous cost and, in some instances, could prove fatal to the enterprise.

The criminals want to steal money and information. They want to steal both your personal and your company's financial assets. They want to inject ranomware into your company systems and shut them down until they get paid. They hope to use your personal devices and home network to acquire your passwords. They also take advantage of neglected cyberprivacy to steal your identity along with your credit, health insurance and tax returns.

The good news is that protecting you and your family from cyber risks is not very complicated. However, the process includes several time-consuming steps that need to be updated regularly and consistently.

This document provides a step-by-step process on what you need to do. It shows what technology you will need and how to use it, along with a series of commonsense steps to create a personal digital security structure. It also describes in detail what you will need to do to manage your ongoing personal cyber risks.

That said, *everyone* online at some point will be hacked and/or have a portion of their identity stolen, *regardless of what they do*. Cybercriminals have immense resources and are backed by nation-states such as Russia, Iran, China, and North Korea.

The objective in taking these measures is to compartmentalize your information and make yourself a much less attractive target and reduce both the frequency of breaches and the damage that they create.

Creating a Personal Digital Security Structure

Necessary technology

Three types of widely available technology are needed to create a personal digital security structure:

(i) Password manager

A password manager is encrypted software that stores passwords for each of your online accounts.

(ii) Virtual private network (VPN)

A virtual private network or "VPN" is software that encrypts your online traffic. It both prevents others from seeing what you are doing on your device and websites from identifying and tracking you.

(iii) Private email

A private email is different than Outlook, Gmail, AOL, etc. because (as its name implies) it is not automatically read and mined for data. However, it does not replace your existing, daily-use emails. Rather, it is used to provide materially greater cybersecurity for both the double authentication feature that certain online accounts offer as welll as the ability to reset one's passwords.

Numerous companies offer versions of each of these three technologies. However, it is important to carefully diligence them because some of these companies are backed by China, Iran or Russia (i.e., where most cybercriminal organizations are based.) There are also others (in particular, low cost or free ones) that you want to avoid because they collect and sell your information.

Seven steps to set up your personal digital security structure

Once you have the necessary technology, there are seven steps in setting up your personal digital security structure:

(i) Install a VPN, password manager and private email on each device.

Each of these technologies should be installed on every smart phone, laptop and desktop computer and tablet. This is relatively easy and take only a few minutes for each device.

(ii) Populate password manager with online accounts and resetting their passwords.

Every online account should be added to the password manager and their passwords should be reset using unique, randomly generated 15 to 20 alphanumeric character passwords. Most password managers include a feature that allows you to generate these kinds of passwords.

Certainly, the time involved in completing this step depends upon the number of online accounts. However, for a typical family this should take about twenty to twenty-five hours to complete.

(iii) Engage privacy settings on online accounts.

Doing this is essential to guarding your digital privacy, which protects you and your family from both identity theft and online predators. Most online accounts have privacy settings that enable users to opt out of their data collection efforts and limit who else can access your account information.

It takes most people about forty hours to complete this process. Because collecting and selling user information is the core business activity of these companies, they intentionally make it burdensome to do this. It typically involves navigating a maze of multiple web pages to determine which settings to turn on for each accounts.

(iv) Engage double authentication settings on online accounts.

Many online accounts have an additional layer of security which, if engaged, requires a user to provide two forms of authentication to log in. Taking this step is essential to reducing the likelihood of the account being breached. Although some sites require that a mobile device be used when providing a second form of authentication, it is preferrable whenever possible to instead use a private email because cyber criminals can easily "spoof" or hijack mobile phones.

Completing this step is likewise dependent upon the number of accounts and, which of those offer a double authentication security feature. However, in our experience it typically takes ten hours.

(v) Engage privacy and security settings on devices.

Several privacy and security settings should be engaged on each device. As part of this, it is important to turn on the ability to wipe a device remotely should it be lost and to activate the necessary settings to prevent apps on the device from gathering and selling your information. Likewise, it is essential to engage the necessary settings to prevent the device and third-party software from automatically copying and storing passwords and to prevent apps from turning on the device's microphone and camera without your permission.

The amount of time involved in this process is dependent upon the number and types of devices and how familiar one is with the settings. In our experience, completing this for a family that has six devices will take about five hours.

(vi) Engage the privacy and security settings on Web browsers and search engines.

When you activate your device privacy and security settings, it is also important to engage the numerous privacy settings on your Web browsers and search engines. Unless you engage these settings, browsers and search engines will track your online activity and gather large amounts of personal information that will be sold to third parties.

This process typically takes about three to five hours to figure out and complete.

(vii) Ensure each device has up-to-date anti-virus software.

At some point, all devices become infected with malware. Ensuring that each device has current anti-virus software is analogous to keeping one's vaccinations current.

<div style="border:2px solid blue; padding:20px;">

Don't Waste Your Money on Online Identity Protection Services

Many companies offer identity protection services which purport to protect families from cyber risks. However, it is important to understand what they do and why it provides very little protection.

More specifically, these services are analogous to backward looking radar — they do little to nothing to prevent you from being hacked or having your identity stolen. Instead, they just alert you when it has happened. Their services also largely ignore cyberprivacy, which is critical to protecting your family's physical safety.

Many people buy them because they include either insurance or "guarantees" to reimburse up to $1 million of costs in the event of hacking or identity theft. However, the terms of these agreements often make collecting on them very challenging.

For example, there is typically an exclusion of liability for the insurer in the event of simple negligence by the user, a very low legal threshold to prove. Some even limit the amount of their reimbursement for attorneys to as little as $120 per hour and $80 per hour for accountants.

They also are often structured as umbrella policies — i.e., one must first sue and collect from everyone else involved, and only then try to collect the difference from the insurer. The costs of this additional layer of litigation are potentially much greater than any amounts that the client might ultimately recover from the insurer.

</div>

Three Part Process to Manage Ongoing Cyber Risks

Creating a personal digital security structure is only the first step. Protecting you and your family also requires an ongoing process for managing your cyber risks over time.

This process has three parts:

1. Detecting and quickly responding when you are hacked and/or have your identity stolen,

2. Systematically updating your protection, and

3. Avoiding making yourself an attractive target for cybercriminals.

Three Steps for Detecting and Quickly Responding to Breaches and Identity Theft

(i) Subscribe to a Dark Web monitoring service.

The Dark Web is the part of the Internet where stolen information is sold. Several companies have the special technology required to access the Dark Web and many offer subscription services to alert you if any of your information is for sale.

(ii) Retrieve and review annually credit reports for your entire family.

Reviewing your credit reports annually is the best way to detect potential identity theft. Each of the three largest credit monitoring bureaus are required to provide free copies. Any abnormalities that appear on them often indicate that someone has stolen your identity. It is also important to check annually to see if there are credit reports for your underage children. If one exists, it often means that someone has stolen their identity.

(iii) Be prepared to quickly address stolen information or identity theft.

Critical to minimizing the damage resulting from either a breach or stolen identity is quickly taking steps to mitigate the problem once it is detected. The steps may be as simple as changing a single password or as complicated as having to make filings with multiple governmental agencies, companies, credit bureaus and law enforcement organizations. In certain circumstances, it might also require freezing or limiting credit and transferring assets to new accounts.

Three Aspects to Systematically Updating Your Protection

(i) Review your digital footprint at least annually.

Everyone should review annually what they are doing online, their devices, and the software they are using to determine what elements of their digital security structure need to be updated. This includes the apps, online accounts, devices, and other technology they have added as well as those they no longer need.

(ii) Update your protection annually.

Unless all aspects of a cyber structure are kept current, the entire structure quickly becomes ineffective. Online accounts regularly change privacy and security settings and need to be updated. Privacy and security settings for new devices, new online accounts, and apps also need to be enabled.

(iii) Keep your family informed and educated about new cyber threats.

No different than any other risk management program, education plays a key role in managing cyber risk. Parents and children need to be informed and educated about ongoing and recently identified threats and risks.

Eight Ways to Avoid Making Yourself an Attractive Target for Cybercriminals

(i) Never link your work and social media accounts

Cybercriminals recognize how vital your company's online presence is to the marketing of your business. Thus, regularly target business owners' social media accounts. If they can take control of it, they can force you to choose between paying ransom and shutting the accounts down and having to rebuild your business' online presence.

Additionally, if they successfully breach a work social media account linked to a personal account, they will have access to an immense amount of information about you and your family that can be used to steal your and your children's identities.

(ii) Never link your business and personal banking and custodial accounts

A breach can quickly go from a bad event to a catastrophic one if cybercriminals can get into both your work and personal financial accounts. For example, the FBI has reported that cybercriminals are increasingly stealing personal devices with their passcodes at restaurants and bars. They will memorize passcodes as they are being entered and then later distract and steal the device from an unsuspecting owner. They then will very quickly change the device's passwords to lock out its owner and use it to steal money from bank and custodial accounts. If a separate password is not required to access work accounts, the amount of potential loss increases geometrically.

(iii) Minimize your smart home technology.

Houses with smart home technology (i.e., digital light bulbs, security cameras, smart coffee pots, smart door locks, etc.) are the preferred targets for cyber criminals. Why? Because it is often very easy to hack. One need only breach a single device to compromise the entire network, and everything connected to it. Thus, it is important to limit your smart home technology to only what is essential and to secure each device with a unique and sophisticated password.

(iv) Never use personal devices or personal email for work

Most personal devices and email accounts typically have a fraction of the cyber security protections of work devices and email accounts. Additionally, unless all necessary privacy and security settings have been engaged, the device will have recorded every online account that you have accessed as well as the associated password.

Consequently, cybercriminals regularly try to breach the personal devices and email accounts of business owners either through WI-FI or with malware. Their goal is to copy passwords that will them allow to breach company systems. They also hope to find in personal email accounts confidential work information.

More problematic, a virus on a personal device can infect work systems should it be connected to company network. Such viruses will allow cybercriminals to steal passwords and personal information as well as to potentially take control of company systems.

(vi) Always wipe lost and retired devices.

Your devices store immense amounts of your information. Wiping lost or retired device memory (including computers, smart phones, tablets, home assistants and leased autos) is critical to protecting both your cybersecurity and cyberprivacy.

(vii) Use USB blockers with rental cars and charging stations.

Whenever a device is plugged into a public charging station or a rental car, information is downloaded almost automatically from the device. In certain circumstances, malware is also uploaded. Using a USB blocker (a small, inexpensive device that you attach to your power cord) prevents this from happening.

(viii) Turn off Bluetooth when you aren't using it.

Bluetooth allows anyone proximate to you to access information on your device.
For example, you may be working on a laptop at a cafe or hotel. Anyone proximate to you can see virtually into your device unless you have turned off your Bluetooth.