What are you doing to actually protect yourself?

Print an updated copy of this packet by going to rowleyservices.com Feel free to share with friends and family.

Who does this affect? EVERYONE

Since 2017 I have been setting up Two-Factor Authentication (2FA) for every client that I have helped. This has completely stopped all account takeovers for those clients, but 2FA is only part of what is needed for security. I have put together this small packet and checklist as a way to help my clients actually protect themselves from the many types of digital and financial disasters. I usually set up most of this for my clients, but I give this packet out as a checklist for anyone that wants to attempt it themselves.

Unfortunately, there are many misconceptions about Account Security and Personal Information Security. Many believe that they can't do anything at all to protect themselves or that paying another company for a VPN / "privacy" monitoring or cleanup will fix the issue for them. Don't fall for emails that say your info was found on the **dark web**. You cannot remove your info from the dark web. Follow the FULL-PAGE checklist to protect your accounts and personal information.

Computer Basics Overview

SECURITY & BACKUP FIRST, PRIVACY SECOND!

- ▢ **Data Backup** in case of data loss. It happens more often than people realize.
- ▢ **Account Security** using 2FA to keep the hackers out of your main online accounts and financial accounts.
- ▢ **Transaction alerts** / notifications to know if someone makes a charge using any of your accounts.
- ▢ **Personal Information Security** to stop identity thieves from using your personal info that they already have.

  Freeze your credit with the 5 credit rating bureaus. Keep track of your login information on the provided page.

  In addition, you should place a fraud alert AFTER you have frozen your credit with each of the 5 sites.

  Understand that A FRAUD ALERT will only last ONE YEAR.

  Credit monitoring will not stop identity thieves, and it is NOT the same as actually freezing your credit.
- ▢ **Federal Tax Filing Protection** requiring a PIN (Identity Protection / IP PIN) to stop fraudulent filing of your taxes.

Don't assume that you are smarter than the scammers and thieves. Protect yourself.

Common Misconceptions:

They already stole my personal info, so now it doesn't matter.
Yes, your personal information has already been stolen. However, by protecting your credit and securing your accounts, you can prevent account takeovers, future data / information theft, and bad credit. You can also prevent your info from being used to create new credit in your name, which usually takes 1-2 years to deal with once it happens.

My bank is really good about reimbursing me if someone steals my money.
Banks are usually good for reimbursing you if your *credit card* is used by someone else, however, financial institutions generally will NOT reimburse you if you are scammed or if money is stolen out of your account.

My bank / financial institution has really good security. My account is protected with my "face".

- Do not assume that your account is protected by a scan of your face or finger. A face scan (FaceID) just allows you to not have to type your username and password every time on a device that you have used in the past.
- Most financial institutions do have decent security; however, this does not mean that it's even enabled for your account.
- Bank of America accounts do NOT have Two-Factor Authentication (2FA) enabled by default, Chase Consumer accounts do have 2FA enabled by default. Many financial institutions require the user to setup 2FA themselves. 2FA is extremely important, but it does not stop users themselves from being scammed. Fraudulent credit card charges are often reimbursed, however, **financial institutions generally will NOT reimburse you if you are scammed or if money is stolen out of your account.**

I don't have a lot of money, so I wouldn't care (or they wouldn't target me).
They target EVERYONE. If you truly wouldn't care if someone stole ALL of the money that you have then you might as well donate your money to a good cause. None of my clients have ever been ok with ANY amount of money being stolen from them. Remember, it's easier and quicker to protect your data and accounts than it is to deal with a disaster later.

I don't do any online banking.
Yes, this still affects you. Scammers use your info to create online banking profiles in your name. With that online profile they can access your bank account and credit and debit card numbers without you even knowing, then they make charges to your account.

Computer Basics Checklist & Reminders

Data Security & Backup:

- ☐ Sign up for Secure Backup Service: visit rowleyservices.com/support for a free trial & setup info.
- ☐ Consider occasional full backups. If you want local backups (to an external drive) or occasional full backups, ask me.
- ☐ Call right away if you get a virus. Stop using your computer. Hackers use viruses to steal logins and financial info.
- ☐ Keep ALL of your data on your computer, and not on external drives or USB / thumb drives, CD's, etc. Do not trust cloud service providers as your main and/or only location for your photos and data. Cloud storage is not backup.
- ☐ Ask me about getting your pictures from your phone to your computer. Don't rely on Apple or Google as a backup.
- ☐ Ask me about getting your computer drive protected with Backup & BitLocker to protect the contents of your data.
- ☐ Ensure you have a phone PIN (Passcode) and a computer PIN (with matching password), written in your password book.

Account & Personal Information Security:

- ☐ **Secure main accounts** using two-factor authentication (2FA). Hackers do far more damage than people realize until it happens to them. It's easier and smarter to protect your accounts now and not regret it later. Ask about Account Security. Microsoft, Google, and Apple should have at least three or four phone numbers added for 2FA.

  ☐ Email, ☐ Apple, ☐ Google, ☐ MSFT, ☐ Amazon, ☐ Facebook, ☐ Phone Provider, ☐ Yahoo,
  ☐ BackBlaze (Online Backup), ☐ Banks, ☐ Investment Accounts, ☐ PayPal, ☐ eBay, ☐ Comcast

- ☐ **Freeze your credit** and get a locking mailbox. ID thieves use stolen info and mail to start new credit in your name. Fill out the attached template with directions to keep track of the 6+ different accounts PER PERSON. Understand that your personal info has already been stolen, it is only a matter of time before scammers will use YOUR info. Credit monitoring will NOT stop identity thieves and is NOT the same as freezing your credit.

- ☐ **Sign up for a yearly IRS Identity Protection PIN** (visit irs.gov, use login.gov) to stop fraudulent filing of your taxes.

- ☐ **Turn on EVERY transaction alert** / text message notification for EVERY Credit Card, Debit Card, Checking Account, Savings Account, Investment Account, etc. Set the notification limit to $1 so you will be notified of EVERY transaction. Enable both text AND email notification for abnormal transactions such as out-of-country charges, ATM withdrawals, wires, etc.

- ☐ **Unsubscribe from unwanted emails** to reduce the amount of junk you have to delete. This can also help reduce the amount of spam and phishing emails that try to trick you into giving up your account credentials. Do not open emails in your junk or spam folders. Unsubscribe from about 20 - 30 per day.

Scams & Device Security:

_____ I will NOT "google" or search for phone numbers for customer service.
_____ I will NOT allow strangers or scammers to remote control my computer.
_____ I will NOT fall for calls or fake emails from Microsoft, Amazon, Norton, etc.
_____ I will NOT SHARE account info, passwords, or security codes over the phone.
_____ I understand that VPNs are a form of PRIVACY and will NOT secure my accounts.
_____ I understand that bitcoins, cashier checks, and gift cards are often used by scammers to steal money.
_____ I understand that if I change my cell phone number I will be permanently locked out of some accounts.
_____ I will not withdraw cash from my bank even if directed by a scammer that is acting as someone from my bank.
_____ I understand that searching can lead to virus sites. I will use BOOKMARKS and the ADDRESS BAR CORRECTLY.
_____ I will use Chrome and the built-in Chrome Password Manager, so I don't type my passwords into fake websites.
_____ I understand that if a friend requests me to buy a gift card via email or phone, it IS a scammer, and not a friend.

Chrome Browser, Password, & Other Reminders:

- ☐ Keep track of all your usernames and passwords ACCURATELY in your password book.
- ☐ Stop changing your passwords. Keep track of all your usernames and passwords ACCURATELY in your password book.
- ☐ DO NOT USE YOUR PHONE NUMBER as your USERNAME for sites like Google, Microsoft, or Amazon, etc.
- ☐ When signing into your various websites, use Chrome Bookmarks Correctly and use your saved usernames and passwords.
- ☐ Use an add block program within Chrome (Add Block Plus). Never click on an advertisement, or any link with these labels: Advertisement, Ad, Sponsored, Promoted, Partner, etc.
- ☐ Call right away if you get a virus. Stop using your computer. Hackers use viruses to steal your logins, bank, and CC info.
- ☐ Call me BEFORE purchasing a new Phone or Computer. I will help you find the best deal.
- ☐ Take Pictures of any Error Messages.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring

Updated: 11 February 2025 Visit RowleyServices.com for an updated copy. Password & Tutorials Packet

Phishing Emails & Scams

Remember: NEVER BUY GIFT CARDS or Bitcoins

Oops! It looks like you got tricked by a scam or phishing email.

☐ I have read and understand.

Name: _____

Date: _____

It is important to understand that there is no ONE way to tell if an email is legitimate, however, there are many ways to know if the email is a phishing attempt or scam.

There are several ways to tell if an email is a phishing attempt or scam:

1. **Check the email sender's EMAIL ADDRESS (not just the name):**
   - Check the EMAIL address of the SENDER. IT IS A SCAM if it's from a random email address (@hotmail.com, @gmail.com, @outlook.com, etc.).
   - Just because an email address LOOKS legitimate, does not mean that the email is from that sender or safe.
   - So, if an email address looks correct, DO NOT TRUST IT, it still could be a scam.

2. **Check the content of the email:**
   a. Emails threatening to close your account.
   b. Emails urging you to sign in or verify your account.
   c. Emails urging you to update or change your password that is about to expire.
   d. Emails about shipments or packages.
   e. Emails about getting a refund for a service or product.
   f. Emails that have "attachments" that are actually just links to another site.
   g. Emails threatening that you will be charged or that you were already charged.
   h. Emails with links to follow. It is generally advised to NOT click ANY links in emails.
   i. Emails requesting you to confirm your account details to UNLOCK your account.
   j. Emails urging you to "take action" before a certain date or time (usually within 24-48 hours).
   k. Emails from PayPal, Microsoft, Google / Gmail, Norton, McAfee, etc. are most commonly sent by scammers.

3. **Do you even have "that" service or product?**
   - Many people are tricked into opening emails and following links for services that they don't even have. People who get scammed often say: *"I got an email from McAfee about a bill / charge, but I don't have McAfee. So, I opened the email to make sure they didn't have my credit card info and that they weren't going to charge me".* DO NOT FALL FOR THIS. This is exactly how the scammers want you to respond.

4. **Links in emails:**
   - Most phishing and scam emails have phone numbers to call or links to click (some just want you to reply via email to them).
   - On the computer you can use your mouse to HOVER OVER THE LINK then the **FULL and ACTUAL** link address will appear (usually in the bottom left-hand corner of the screen).
   - If the link address looks fake (ex: microsoft-email.com/sign-in/) then you know the email is a scam.

Remember: Use this info to know that the email is a scam (none of this will tell you that the email is legitimate or safe).

There are tons of new types of phishing and scam emails that are being created daily. It is usually better to be cautious and assume that it's a scam first, then ask for help if you are not 100% certain.

None of the large companies like Microsoft will ever "lock you out of your account", or "charge you" if you don't follow the email directions within 24-48 hours. NONE OF THEM USE TIME LIMITS LIKE THAT.

Don't fall for emails that say your info was found on the **dark web**. You cannot remove your info from the dark web. Follow the instructions in this packet to protect your accounts and personal information.

If you have an email that you really think is legitimate, but you are still unsure, just CALL ME.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring

BROWSER REMINDERS

BOOKMARKS – ADDRESS BAR – SEARCHING

Use the Bookmarks Correctly:

Bookmarks should be made for any website that you regularly visit.
Label / NAME your bookmarks correctly to help you remember the actual address of the bookmark. For example, your bookmark for amazon should be named “amazon.com” not “amazon” or “amazon prime”. The website ADDRESS for the bookmark should also be “amazon.com” not “amazon.com/sign-in”, this will ensure that the bookmark always works in the future in case they change their sign-in page.

Use the Address Bar Correctly:

The address bar at the top of your browser is also a search bar. While you can type anything into the search bar, you shouldn’t. If you don’t already have a bookmark for a certain site, You SHOULD type in the actual address then press the ENTER KEY on the keyboard. For example, if you are visiting your health insurance provider for the first time and have paperwork that shows their website address, type the address in the address bar and press the ENTER KEY. Do NOT use your mouse to click a search suggestion from the drop-down list, as this will just do a search which increases your risk of getting a virus. For example, do not type in Rainier Health, instead type in rainierhealth.com then hit the enter key. This will take you directly to the site.

Use the Search Bar Correctly:

If you haven’t already bookmarked your site and also don’t know the exact address, then consider searching as your last option. The address bar also functions as a search bar. Using google search or any search engine to get to a known website greatly increases your risk of getting a virus.
Keep your searching to a minimum and pay attention to the site address before clicking links. Sites commonly known to have virus’: Political, religious, game sites, recipe sites, shopping, social media, etc.

Browser Protection:

Call right away if you get a virus. Stop using your computer. Hackers use viruses to steal logins, credit card info, and bank and financial info. Do not assume that just because you restart your computer or can’t see a virus screen anymore that the virus is suddenly gone. Get your computer checked ASAP.

Use an add block program within Chrome (Add Block Plus).

Never click on an advertisement, or any link with these labels: Advertisement, Ad, Sponsored, Promoted, Partner, etc.

Credit Freeze

Freeze your credit and get a locking mailbox. ID thieves use stolen info and mail to start new credit in your name. FREEZE your credit (do not sign up for monitoring). Credit monitoring will not stop identity thieves and is NOT the same as actually freezing your credit. Do **not** sign up for paid monitoring services or any trials for monitoring.

Make sure you go DIRECTLY to these sites. DO NOT GOOGLE THEM. Then look for the links to "Freeze Your Credit".

☐ **Enable <u>EVERY</u> transaction alert for <u>EVERY</u> credit & debit card, checking, saving, and all financial accounts.**

Experian.com Multiple / Weekly Credit Report checks per year.

Username:		
Password:	☐ 2FA	☐ 2FA
Q & A:		
PIN: (4 Digit):		
Date Frozen:		
Notes:		

Equifax.com Six Free Credit Reports per Year.

Username:		
Password:	☐ 2FA	☐ 2FA
Q & A:		
Date Frozen:		
Notes:		

Transunion.com Transunion lets you check your Credit Report once every 24 hours.

Go to transunion.com THEN click "Member Login", then choose "Service Center."
The "Credit Monitoring" button on the main page is for their paid services ONLY.

Username:		
Password:	☐ 2FA	☐ 2FA
Q & A:		
PIN (6 Digit):		
Date Frozen:		
Notes:		

ChexSystems.com & OptOut - PRINT your PIN and add it to the box below.

Username:		
Password:	☑ Auto 2FA	☑ Auto 2FA
12 Digit PIN:		
Date Frozen:		
Notes:		

Innovis.com – Innovis will mail you a PIN via USPS.

MAILED PIN:		
Date Frozen:		

OptOutPrescreen.com (or set via ChexSystems on Menu Bar) – Check every Five Years

Opt-Out Date:		