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 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 or that paying another company for monitoring or cleanup will "fix" the issue for them. Don't fall for emails that say your info was found on the **dark web**. <u>You cannot remove your info from the dark web.</u>
Follow the checklist to protect your accounts and personal information.

This Packet Covers:

- **Data Backup** in case of data loss. It happens more often than people realize.
- **Device Security** to reduce viruses and keep hackers off of your computer.
- **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 is NOT the same as actually freezing your credit.
- **Federal Tax Filing Protection** requiring a PIN (IP PIN) to stop fraudulent filing of your taxes before you file yourself.

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

Common Misconceptions:

They already stole my personal info, so now it doesn't matter.
Yes, your personal information has likely 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, <u>financial institutions generally will NOT reimburse you if you are scammed or if money is stolen out of your account.</u>

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 enable 2FA themselves. 2FA does not stop users themselves from being scammed. Fraudulent credit card charges are often reimbursed, however,
  <u>financial institutions generally will NOT reimburse you if you are scammed or if money is stolen out of your account.</u>

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

Ask me about getting these set up.

Data & 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, let me know.

☐ 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 to keep your photos.

Account & Personal Information Security:

☐ **Secure your main accounts** using two-factor authentication (2FA). Hackers do far more damage than people realize until it happens to them. It is easier and smarter to protect your accounts now so that you don't regret it later.
Ask me about Account Security. ☐ Email, ☐ Apple, ☐ Google, ☐ MSFT, ☐ Amazon, ☐ Facebook, ☐ Yahoo, ☐ Comcast ☐ BackBlaze (Online Backup), ☐ Banks, ☐ Investment Accounts, ☐ ALL Transaction Alerts, ☐ PayPal, ☐ eBay.
Microsoft, Google, and Apple should have at least three or four phone numbers added for 2FA.

☐ **Freeze your credit** and get a locking mailbox. ID thieves use stolen info and stolen 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 by identity thieves, it is only a matter of time before they will use YOUR info. Credit monitoring will NOT stop identity thieves and is NOT the same as actually freezing your credit.

☐ **Sign up for a yearly IRS IP PIN** to stop fraudulent filing of your taxes before you get a chance to file your taxes yourself.

☐ **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 withdrawal's, 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.

Chrome Browser & Password Reminders:

☐ 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 (uBlock Origin or 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.

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 VPN's are a form of PRIVACY and will NOT secure my accounts.
_____ I understand that if a friend asks me to buy a gift card, it IS a scammer, and not my friend.
_____ I will not withdraw cash if directed by a scammer that is acting as someone from my bank.
_____ 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 understand that searching increases viruses. 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 sites.

Other Reminders:

☐ Take pictures of any error messages.

☐ Call immediately if you have or think you have a virus, do not wait.

☐ Call me BEFORE purchasing a new phone or computer. I will help you find the best deal.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring – Updated: 10 Nov 2024

Phishing Emails & Scams

Remember: NEVER BUY GIFT CARDS or Bitcoins

☐ I have read and understand.

Name: _____

Date: _____

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

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:**
   1. Emails threatening to close your account.
   2. Emails urging you to sign in or verify your account.
   3. Emails urging you to update or change your password that is about to expire.
   4. Emails about shipments or packages.
   5. Emails about getting a refund for a service or product.
   6. Emails that have "attachments" that are actually just links to another site.
   7. Emails threatening that you will be charged or that you were already charged.
   8. Emails with links to follow. It is generally advised to NOT click ANY links in emails.
   9. Emails requesting you to confirm your account details to UNLOCK your account.
   10. Emails urging you to "take action" before a certain date or time (usually within 24-48 hours).
   11. 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 email 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. 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 – Updated: 10 Nov 2024

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.
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.

STOP CHANGING YOUR PASSWORDS

Keep track of all your usernames and passwords ACCURATELY in your password book (or an excel sheet if you are good at keeping it up to date).

When signing into your various websites, use Chrome to save and autofill your usernames and passwords (make sure you have 2FA enabled on your google account). The chrome password manager is built into Chrome and syncs your login credentials between all your devices: PC’s, Mac’s, iPhone, Android, etc.

If you forget a password, then fall back to your password book. If it isn’t working then you are likely either on the wrong website (possibly getting scammed), or you didn’t follow the step above to KEEP TRACK of your passwords in your password book.

Keeping track of your passwords is easier than resetting them as resetting your passwords will often cause syncing issues on other devices.

Remember that some companies like Microsoft, Apple, and Amazon have multiple services yet still use the same login for all of their services. For example: Your Apple ID is for iTunes, iCloud, Apple ID, app store, FaceTime, iMessage, etc., and should be saved under “Apple ID”. Any other usernames on other pages should point back to “Apple ID”. For example, in your password book the “I” page should not have iCloud, iMessage, or iTunes, but they can have “SEE APPLE ID” next to any of those to remind you to only keep track of your Apple ID in ONE PLACE ONLY. The same is true for your Microsoft Account which includes services for Hotmail, MSN, Outlook, Skype, Xbox, Word, Excel, etc.; all of these should point back to “Microsoft Account”. The same is also true for Amazon. Amazon Shopping, Amazon Smile, Prime, Kindle, Alexa, Audible, etc. all use the same login info; “Amazon.com”.

Keep a written record of your usernames and passwords correctly and in ONE PLACE ONLY (your password book). This will help you to NOT get locked out of your accounts.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring – Updated: 10 Nov 2024

Credit Freeze & Monitoring Services

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 EVERY transaction alert for EVERY 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 – Download and PRINT your PIN and add it to the box below.

Username:		
Password:	☐ 2FA	☐ 2FA
MAILED PIN:		
Date Frozen:		
Notes:		

Innovis.com & OptOut

10 Digit PIN:		
Date Frozen:		

OptOutPrescreen.com (or set via innovis.com) – Check every Five Years

Opt-Out Date:		

How to get pictures to your computer via Dropbox:

Open Dropbox on your phone often (once a week or so), or after you have taken photos that you want on your computer.

DO NOT DO ANYTHING IN DROPBOX, just open Dropbox and let it run automatically.

Do not attempt to manually upload pictures.

1. Plug your phone into POWER (optional).
2. Open Dropbox on your phone (keep open for 5 – 15 minutes).
3. DO NOT DO ANYTHING ELSE (NO MANUAL UPLOADS).
4. Repeat weekly or monthly.

Keep your computer ON so that your photos will sync to your computer. Your photos will sync from anywhere in the world, you do not need to be at home (Wi-Fi is recommended).

If you see any messages that **Dropbox is full**, first **restart** your computer then wait about 30 minutes and open Dropbox on your phone again. If you continually get any messages about Dropbox being full, call Derek.

The number of photos in Dropbox will eventually get down to zero, and it will say "All done backing up". **When you see that message, you can close Dropbox.**

Your photos will eventually be sorted into the Picture folder by year and date.

If you need to see new photos that recently synced to your computer, they may be visible in the "Camera Uploads" folder for a few hours until they are automatically sorted into the pictures folder. It is usually best to just wait until the next day to see your pictures in the pictures folder.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring – Updated: 10 Nov 2024

iPhone users that use a Windows PC.

Apple Photos (and documents) in the Cloud: Apple recently started moving photos and videos taken with an iPhone to iCloud (Apple's online storage / cloud). **In the process they have automatically enabled settings that reduce the quality of the photos and videos stored on your iPhone**. Here's how it works: You take a picture; your iPhone saves a copy of the photo or video at a much lower resolution to help save space on your phone. Apple sends the full quality picture or video to their servers. Because the image or video on your phone is low quality, anything that you then do with that photo or video will always be at a reduced quality, unless you change the setting (more info below).

Apple's goal is to get you to use their paid iCloud service, which isn't necessarily bad, but I don't recommend it for multiple reasons. Mostly because of the simple fact that I've seen many people lose thousands of photos and documents, usually not noticing until months or years later, when it's too late to even attempt any type of recovery. Accounts also get hacked. Not only is this a privacy issue, but you also risk getting locked out of your own account, once again, losing your documents and family memories that you trusted to the "cloud" (a server that you have absolutely no control over).

Google Photos and Amazon Photos Users: While these are great services, they do not save your full quality photos or videos. In addition, photos are copied from your iPhone, if your iPhone doesn't have the original high-quality photos to begin with, there is no way that Google or Amazon will have your original / high-quality photos and videos. Even if you change your iPhone Settings, Google and Amazon will reduce the quality of their copy by default.

Do not trust cloud service providers as your <u>main</u> and/or <u>only</u> location for your photos and data.

Below are my data storage recommendations. Please call to get these set up correctly:

1. iPhone users should change the settings so that pictures and videos are not resized. The steps are easy but depending on how many photos you take and when Apple changed the settings on your phone, you may not have enough free space on your phone for the original / high quality photos and videos (always pay the extra $200 for the iPhone model with more storage space). **<u>If you have questions about this process, please call.</u>**
   - ☐ To check and change these settings, go to the iPhone "Settings" app. Click your name at the top. Tap "iCloud". If "Photos" is off, then don't do anything else. If "Photos" is on, then follow these steps: Tap "Photos" then tap "<u>Download and Keep Originals</u>". This will start the process of downloading your full quality photos back to your phone. <u>This process can take anywhere from a few minutes to a few hours or days</u> depending on the number of photos, the speed of your phone, and the speed of your Wi-Fi connection.
   - ☐ Open the "Photos" app. Tap the "Photos" tab at the bottom left. Scroll to the very bottom then scroll some more. At the **very very very** bottom of the photos, you should see the number of photos and videos along with the download process if it is still downloading the original high-quality photos from iCloud. Original photos will only download over Wi-Fi, so make sure you are connected to Wi-Fi.
   - ☐ Once you have checked that all photos have downloaded at the very bottom of the Photos app, you can go back to the "Settings" app and turn off "iCloud Photo Library".
2. Sign up for **<u>Backblaze - Online Backup</u>** (PC & Mac). Visit <u>RowleyServices.com/Support</u> for a free one-month trial.
   - Mac users should always have a TimeMachine backup drive setup. Consider TWO drives for dual backup.
   - Online Backup is cheaper than attempting to restore your data from a failed hard drive.
   - Online backup is $190 for TWO years, which is about $7.50 a month (well worth it).
3. Use Dropbox to get your photos to your computer. Ask to get this setup correctly and so that it is fully automatic. My favorite feature of Dropbox is that all your photos and videos will be automatically named with the date and time they were taken. No more "IMG_6896.jpg".
4. Keep <u>all of your data</u> ON your main computer (Documents, Pictures, Music, etc). MOVING your data to an external hard drive is NOT a backup. With all your data on your computer use online backup. If you already have an external drive, call me and I can help set it up to AUTOMATICALLY backup everything to a different drive. Manual backups (copy and paste) are NEVER recommended.
5. Use iCloud Backup for your iPhone. To Set and Check iCloud Backup open "Settings", tap your name at the top, tap iCloud, tap iCloud Backup, enable iCloud Backup. Remember to check your iCloud Backup setting occasionally. The last backup date will appear when checking the settings page. Make sure the last backup is within the last 24 hours.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutoring – Updated: 10 Nov 2024