Staying Safe Online - A Rational Approach
Pam Holland, Founder and President, Tech-Moxie
December 2019
https://www.tech-moxie.com/
Pam (at) tech-moxie.com

We get *many* questions about online security. And we often get brought in to help clean up after an incident of fraud. As a result, we have developed what we consider 'a rational approach' to online security. Rather than focusing on all of the possible risks, we urge our clients to first address factors that present the highest risk. With respect to protecting from online risk, we apply the 80/20 rule. In short, 80% of the risk comes from 20% of the possible causes. In other words, if we just address the top possible risks, we eliminate the most common ways people are victimized online.

We suggest thinking about protecting your data as you might approach protecting your home. We all take reasonable steps to secure our homes; we lock our doors, close windows, and leave lights on. The goal is to *reduce* risk as eliminating risk is nearly impossible. The same is true in our digital lives. Taking small measures goes a long way towards keeping us safe, but it is nearly impossible to eliminate all risk.

Consider your personal risk factors. This is not unlike assessing your home for the risk of a break-in. If you live on the top floor of a high-rise, leaving your windows open does not present the same risk as if you were on the ground floor. With respect to your tech, do you have people regularly in your home that you need to protect your data from? Do you bank online? Do you have sensitive financial or other documents on your computer? Do you only use your computer for email? Do you or a family member have cognitive issues that might make you more vulnerable to fraud?

Based on our experience seeing the aftermath of fraud, taking steps to cover these six items will go far towards your online safety:

1. **Use Unique Passwords.** I know this isn't what many want to hear, but unfortunately, the risk in re-using the same password is increasing. A few years ago, the common advice was to create a unique password that was hard to guess. Today, the risk is not that someone will guess your password - the fraudsters already know it. Large corporate data breaches (e.g., Equifax and Marriott) may have put our passwords into the hands of fraudsters. If you typically use the same password for multiple accounts (and worse if you have used it for years), fraudsters are more likely to be able to access your other accounts. To return to the home analogy, it is as if you have given out your key to numerous people over the years - it's now time to change the locks. Some options:
    - **Use a password manager** - This might mean allowing Chrome or your Mac to save your passwords or using a third-party service like LastPass. I am often asked if they are safe. The only answer that I can really give is that they are safe until they aren't. I have chosen to

allow my passwords to be saved on my Mac. For me, it has reduced my risk (because I don't need to reuse passwords) while (somewhat) saving my sanity. *But a caution: If others have access to your computer, they may be able to view your passwords.*
    - **Write them down -** This works well for many. Of course, it is important to keep the passwords in a safe place.
    - **Develop a unique naming convention -** For example, you might take a short phrase that you will remember then add something unique to that account site.
    - **Make your passwords safer by using two-step authentication -** This is an option in most online accounts (email, Facebook, banking). How does it work? When you log in from a new device or location, you'll be sent a code via smartphone or landline. This makes it harder for fraudsters to log into accounts even if they have your password. To set up, go to the account or privacy/security settings in your online accounts.
2. ***Never* Allow Remote Access to Your Computer** (unless you have sought reputable assistance like from Tech-Moxie 😉). Fraudsters would like nothing more than to gain access to your computer. They pretend to be from Amazon, Microsoft, Apple or another company you know well, offering to "help" you with a service issue. Assume fraud if you get an email, call or computer alert from a familiar company or government name. Once in your computer, they can access accounts and passwords. We have seen quite a lot of damage from these schemes.
3. **Think Before You Click.** Assume links in the email are fraudulent unless you can prove otherwise by checking with the sender. Fraudsters easily create emails that look like they came from a friend, bank or even the government. The email might be friendly (*"Hey, check this out"*) or intended to provoke anxiety (*"your Amazon order for a diamond ring has just shipped"*) or seemingly innocuous ("*your computer needs service"*). Fraudsters are hoping to get passwords or other personal information. Remember, customer service doesn't come to you! Instead of clicking, go to the website directly via the internet.
4. **Beware of Pop-Ups** A "pop-up" is a window or box that opens on your computer - often with a warning. Do not believe pop-up warnings claiming there is a problem with your computer. Never give them remote access. Warnings may claim to be from Microsoft, Apple or another company you are familiar with. What to do? Shutdown and restart your computer and the pop-up should be gone!
5. **Update Devices Regularly.** Companies like Microsoft, Apple and Google lookout for software vulnerabilities that fraudsters can take advantage of. They issue updates to fix these issues. Some devices may be set to automatically update, but others may require you to take a specific action. This applies to computers, tablets and smartphones.
6. **Beware the Telephone.** Scams change but follow common themes. Neither Apple nor Microsoft will call to alert you of problems. Government agencies

such as IRS, Social Security Admin nor the local Sheriff will call claiming you owe money. If you are still in doubt, hang up and call the agency from a number that you have looked up independently.

We hope you find these tips helpful - and as always, we are here to help!