



Bulletproofing Your Digital Identity

Andrew Porter, CISSP®

Your Most Valuable Asset

Your most valuable asset isn't just your portfolio, property, or business interests. Today, your digital identity is what proves who you are when you bank, invest, travel, communicate, and work with trusted advisors. As more of our lives move online, protecting that identity has become central to protecting the legacy you've built.

The good news is that while cybercrime has become increasingly sophisticated and convincing, the most effective defenses have not changed. Cybercrime relies on urgency, fear, and confusion. By contrast, calm decision-making, verification, and a few well-established security practices can dramatically reduce your risk of becoming a victim.

This document provides a clear, practical overview of the most important areas of cybersecurity affecting individuals and families today. It introduces digital identity and outlines straightforward steps you can take to reduce risk and protect yourself from today's most common cybercrimes.

What is a Digital Identity?

Your digital identity is a collection of information that proves you are you in the digital world. It's what banks, investment firms, credit card companies, cell phone carriers, and email services rely on to allow access and approve requests.

Your digital identity consists of a combination of your personal data →

Criminals no longer rely on stolen documents to carry out their crimes. Instead, they rely on stolen information and access that is used to impersonate you online.

Protecting your digital identity is the single most important step you can take to reduce your risk of becoming a victim of cybercrime.



Steps You Should Take

While protecting your digital identity can seem incredibly overwhelming at first, there are some simple, practical steps that you can take to quickly close the door on cybercrime.



Secure Devices – Your phones, tablets, and computers are the keys to your digital identity. Require a PIN, password, or biometric such as face or fingerprint recognition to access your devices. Many devices also include features that can locate, lock, or erase the contents of a lost or stolen device.



Multi-Factor Authentication – MFA is a second form of verification required to confirm your identity before gaining access. Adding MFA to all online accounts that contain sensitive information makes hacking those accounts much more difficult.



Email – Treat unexpected emails with caution – especially ones using scare tactics, fear, or artificial urgency. These emails may contain malicious links that can be used to hack your device, download malware, and bait you into divulging personal information.



Trust But Verify – Unexpected communication by phone, text, or email should always be treated with caution. Never provide access, codes, or personal information unless you are 100% certain the request is legitimate and the person is who they claim to be.



Limit Shared Information – Reducing the amount of personal information you share lowers the risk of becoming a victim of cybercrime. Avoid oversharing travel plans, family details, and financial information. Always shred sensitive documents rather than discarding them.



Callbacks – Scammers often initiate contact using fake phone numbers and email addresses. When you receive an unexpected request, especially one involving money or access, do not respond directly to the message or call. Instead call or email the institution using the contact information listed on their official website.



Trusted Friends & Family – Never take action or make decisions out of fear, urgency, or threatening tactics. Having a trusted friend or family member to consult before acting can help prevent costly mistakes. Fraud succeeds when decisions get rushed.



Technology as a Tool – Criminals are increasingly using artificial intelligence (AI) to impersonate trusted companies and deceive users. If an email, text, or call seems suspicious, verify it through trusted online sources before taking action. A few minutes of research can help prevent identity theft and financial loss.



Identity Protection Services – Consider leveraging a reputable identity protection service as an added layer of security. These services help monitor for signs of identity theft and account compromise, and provide guidance if needed.



Let Experience Be Your Guide – You've spent decades making sound decisions, managing risk, and recognizing when something doesn't feel right. Those instincts remain one of your strongest defenses in a digital world.

Quick Reaction Guide

The previous page has actionable steps to take to stay protected in a world of increasing cybersecurity risk. Below, we've included a quick reaction guide you can reference in the event you encounter a potential scam – so you can make fast, informed decisions with confidence.

Scam		Reaction
Unsolicited phone calls and voicemails	→	Callbacks to trusted phone numbers
Suspicious emails, texts, and social media	→	Non-engagement
Computer and mobile device pop-ups	→	Reboot
Letters or other physical mail	→	Look up contact info online (not on letter)
Family emergency scams	→	Code word and internal communication
Play on emotion (fear, urgency, panic)	→	Stop and consult someone you trust
Credit theft	→	Freeze credit with major bureaus

Stack Financial Management, Inc.

625 Wisconsin Ave
Whitefish, MT 59937
(406) 862-8000

www.stackfinancialmanagement.com