WEALTH FACTORY

A Guide to Cybersecurity and Your Money

A Wealth Factory E-Book

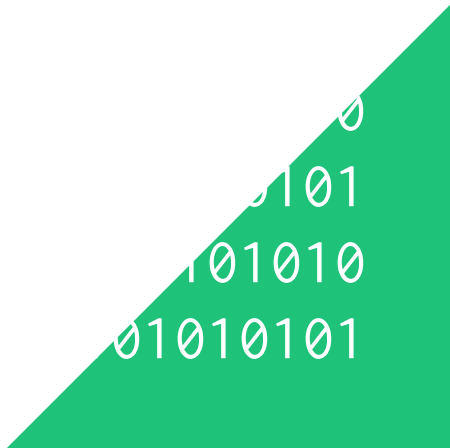
> “Security is going to be the most important aspect of every company on the planet...”

– Leonard Brody for KPMGVoice, Forbes

And while companies struggle to keep up with the security challenges of moving your digital lives online, every day there's another company security breach affecting consumers.

And it can affect your savings, retirement, your bank accounts, credit, identity, and wipe out any hope for leaving a legacy or enjoying retirement, overnight.
Time to tighten some things up, so let's begin...

There’s no need to wipe out your wealth because of a simple security error. It might seem overwhelming securing your financial life from hackers and predators. However, there are a few simple things you can do to keep the bad guys at bay. Make it tough enough and they might just try to find an easier target.



01 Use an encrypted password manager

Throw away those stickies, the notepad, and or that spreadsheet organizing your passwords, and get a password manager like 1password. It's a tool that holds all your passwords securely, meaning you'll never have to remember a bunch of different passwords again. Using the same password for multiple sites, or using a few variations of that password, is a security death sentence. Once a hacker gets ahold of one of your passwords, there's a good chance they can find other accounts you own and get into those, too.

Every month you see in the news that hackers got into Yahoo, Dropbox, LinkedIn, and other big companies and stole millions of users' passwords. All the more reason to use a password manager. Create a new, unbreakable password with a password manager, and sleep well at night knowing you have a leg up on everyone else.

Pro tip: When a company makes you fill out security questions, like "What is your favorite food?" use your password manager to create and save a bogus answer. Using your real answers can make it easy for bad guys to collect enough information about you via other means, that they might be able to access your account just by answering the security questions.

Avoid phishing scams

Spending a couple of minutes getting wise to phishing scams is a lifetime of outsmarting the bad guys. A phishing scam is simply a scheme a bad guy will use to “trick” you into giving him your password or other sensitive information, for example, by presenting you with a login page that looks exactly like one of your own.

If you're not sure if something is a phishing scam, search for it on Google. For example: search the domain a suspicious email came from, or a phone number that claims it’s the IRS. Chances are good that if it's a scam, other people have searched for and reported it online, too. See the resources section of this guide for some scam alert resources.

Pro tip: Don't visit your bank's website by clicking on a link in your email. Bad guys pretending to be your bank is an easy way for hackers to gain access to your bank account.

For more examples, here are a few more tips from the SEC to avoid phishing attacks.

Protect your business checking account from fraudulent money transfers

As reported by NPR: “Cyberthieves steal hundreds of millions of dollars a year from the bank accounts of U.S. businesses.” And believe it or not, if your business checking account gets hacked, the bank can argue that it’s not liable. The bank can even argue that it doesn’t have to pay you back for the loss. It happens more frequently than you’d think.

Think FDIC Insurance would cover the loss? Guess again. It will only cover up to a certain amount. And more importantly, that might not cover the loss of someone hacking into your account, pretending they’re you, and stealing your money. Check with your bank on that insured amount, and if you can avoid it, don’t keep more money in that business checking account than you have to. And of course, beef up your security with a password manager (see #1 in this guide).

Also, implement the other strategies in this guide to decrease the chance of getting hacked.

Use two-factor authentication

(it’s easier than it sounds and it’s totally worth it)

Two-factor authentication simply means that to log into your account, the system verifies you are who you say you are, by doing something like texting your cell phone a verification code. Services like Google, Facebook, Yahoo, and Dropbox allow you to implement it. At Wealth Factory, two-factor authentication is required for everyone’s email accounts. *It’s so important, we even make our mothers do this with their own personal accounts.* Two-factor authentication makes it *much* tougher for a bad guy to get into your account and steal your stuff.

Want to learn more about two-factor authentication? Here’s a great article from Lifehacker on the subject.

05

Have a business?
Protect your business data.

This can be your customer database, or the method that you and your customers send information to each other, or the security of your website.

+ Using a password manager to create and use a strong password, as well as two-factor authentication (when it's available) will go a long way here. And change these passwords regularly. We recommend every 6 months, or at least once per year. It's not a headache when you're using a password manager.

+ For your website, or any other site that you interact with or provide information to, make sure your transactions are secure. You can validate the security of your site by checking to see if there is a green padlock next to the address or that the address is preceded by 🔒 **https**... This indicates that the interaction between your website and your customers is safe from would-be hackers. If your website is not secure, don't panic. Talk to your tech person about securing your site and data.

According to various studies, 62% of cyber breach victims are small to mid-sized businesses, and the average cost of a breach is now at $3.79 million, so it makes complete financial sense to clean up these common security holes.

Watch your nest egg like a hawk

Everything is hackable. In September of 2017, Equifax, one of the largest credit reporting agencies, experienced a massive data breach.

That marks almost the 2 year anniversary of when Dow Jones experienced a data breach. The list of big organizations getting hacked goes on and on. One big systemic hack could send the market flying like a bat out of hell. So if you do have stocks, put stop loss protection on them to protect against a freak crash (though this won't stop all the bleeding in an overnight drop). If you have other assets that you manage online, then read on...

At Wealth Factory, we advocate retiring into your business and into cash flow, not socking away a pile of money for one day, some day, in the hopes that you have enough to retire and live on before you die. But saving is still important. And now that more of your life is online – including your savings or retirement accounts – the last thing you need is a hacker running off with your nest egg.

Again, firm up your passwords here, and enable 2-factor authentication. If your retirement account's online access portal doesn't give you the option to enable two-factor authentication, consider taking your retirement account somewhere else.

07

Move those eggs around

We're actually big fans of the saying, "Put all your eggs in one basket and watch it like a hawk." But we're usually talking about focusing your attention and energy, not fragmenting it across a number of different things.

When it comes to your money, though, keeping all of it in the same account might not be the best idea. It's okay to have some money in a bank account. But there are other secure places to stash some of your wealth as well, whether it's a preparedness stash in a safe, or cash value in a Cash Flow Insurance policy.

These aren't tied to the market or your bank account, so if something catastrophic happens or you're hacked, you won't have lost all your wealth.

P.S. Playing around with cryptocurrencies like Bitcoin and storing them in a digital wallet? A friendly heads up - *digital wallets like Coinbase are not banks, even though they market themselves as banks.* Every day, people get scammed out of their Bitcoin from their Coinbase account. There's no FDIC or way to get that money back. So take some security protocol suggestions from this advice and stick to it, and you'll be on your way to keeping more of your money out of the hands of hackers.

Don’t pick up the phone if it’s the IRS, because it’s not the IRS

The IRS will never call you to demand immediate payment over the phone, and they’ll never email you to verify your identity by asking for personal information. But that doesn’t stop thousands of people from getting defrauded every year in IRS phone and email scams, where bad guys call or email taxpayers, impersonating the IRS and demanding tax dollars.

According to this article on Forbes, “nearly 6,400 victims have collectively paid over $36.5 million to scammers posing as Internal Revenue Service (IRS) officials since October of 2013.”

And according to the IRS itself, 724,000 taxpayers’ information was stolen in a cyber attack on the IRS last year.

Which leads us to Identity Monitoring…

A report by Javelin Strategy & Research indicates that identity fraudsters “have stolen $112 billion in the past six years. That equals $35,600 stolen per minute, or enough to pay for four years of college in just four minutes.”

Even more alarming? 500,000 children in the US are victims of identity theft annually. According to a study by Carnegie Mellon University’s CyLab, children are fifty-one times more likely to be victims of identity theft than adults.

And because people don’t often consider this, you might not find out until years down the road when they apply for their first credit card and get denied because some hacker used up their credit years before. So when do we suggest you start talking with your kids about cybersecurity? Now.

While identity theft protection is not bulletproof, we still suggest signing up yourself, your significant other, and your children; keeping an eye on your credit, and tightening up your online bank account passwords.

You’re off to a great start!

Simply by filling a few simple security holes, you can be light-years ahead of other people. With so much of our lives online these days, it’s important to spend a few minutes on security awareness so you can live the life you love, and not let it be enjoyed by a hacker instead.

Favorite Resources

Favorite Book on Privacy and Security

Future Crimes by Marc Goodman (he's one of the world's leading authorities on global security, and a source of a lot of the facts in this guide)

How to find out if you've been hacked, in seconds

Check if you have an account that has been compromised in a data breach

Note: One of our own researchers for this guide found his own private email address in here.

Extra note: if you find your email address on here, that doesn't mean you need to create a new email address. Definitely change your password on the site that's been compromised. Setup 2-factor authentication on that account if you can. And consider some of the other suggestions above, including changing your security questions to fake answers, and saving them in your password management app.

If someone holds your computer system ransom

Get it back without paying your attackers, at NoMoreRansom.org

Favorite Resources (continued)

Identity Theft Recovery Steps

Identitytheft.gov

What to know and do about scams in the news

Scam Alerts by the FTC

Track local scams in your area, by zip code

Scam Tracker by the BBB

What to do if you've discovered a data breach

https://www.ftc.gov/databreach

A great Twitter account with security resources

National Cyber Security Alliance on Twitter

What is Wealth Factory?

Wealth Factory's mission is to manufacture economic independence for entrepreneurs and business owners. We're committed to helping you keep more of your money, and increase monthly cash flow without having to work harder, take on more risk, or hire a single new employee.

WEALTH FACTORY