How to Protect Your Information Part 1: Structure and Hardening Your Email Accounts

There are two levels of information security that impact your financial well-being and privacy. The first is the security of the server where your data is stored. This includes banks, utility companies, government agencies, hospitals, and email servers. In general, you don't have any control over the security of this information.

This level of data is often probed by hackers seeking large pools of information that can be searched later on for valuable targets such as people with good credit ratings or something else that can be used to advantage by a hacker or identity thief.

The second data security point is your personal account access information. Your email address, passwords, user name, biometric data, and phone number are all within your control. To some extent, you can harden your email structure to ensure breaches at this level, and the institution level do not impact every area of your life.

Most websites that store your financial information let you log in with your email address as your username. From there, a hacker only needs to figure out your password. This is like giving hackers 50% of the data they need to hack your account.

Once your email address is hacked, it becomes easy to find out just about everything going on with financial or other communications that are important to you. At that point, you become an easy target for anyone interested in stealing or damaging your identity for financial or other reasons.

Choosing Email Hosts

Even if you don’t have a lot of transactions, you may need anywhere between 7 and 10 email hosts. While this may seem inconvenient, getting hacked is much worse.

To find email servers, you can do the following:

- Do a web search for free email addresses. Use a range of popular and less popular servers. Don’t underestimate the usefulness of less popular servers. Since there are fewer people using them, they are also less interesting to hackers. On the other hand, their security may not be as robust.
- Purchase separate domains through different web hosts. These domains should be used for email hosting only. Here again, choose between popular registrars and ones that are less appealing. Regardless of the registrar, make sure you understand what type of support they will offer if their servers are hacked and your information is exposed.

Diversifying Email Addresses

One of the most important things you can do is structure email addresses for different kinds of communication and transactions. You may also need to open a range of bank, and other accounts to reduce your risk of exposure from hackers.

- First-level addresses—Use one for each bank you deposit money into. If you have a business, make sure you set up

a similar address for the primary bank where you receive payments.

- Second Level Addresses – a separate email address for each online, or other bank account that you make deposits into from your primary bank account. Make sure you choose a secondary bank where the funds cannot be automatically drawn from the primary bank account if the funds are too low.
- Third Level Addresses – Separate addresses for Paypal or other online processors that you can use as an intermediary between your secondary bank and any trusted site or business where you shop. Make sure funds cannot be automatically drawn from the secondary bank account if funds are too low in the intermediary. If a hacker gets into a merchant account or the intermediary, you don't want to be in a situation where they are able to get at your money in underlying banks.
- Fourth Level Address – A separate address for your utilities, credit cards, and other primary bills. When setting up electronic payments for these bills, make sure you use one of your third-level email addresses. Worst comes to worst, even if they hack your secondary and tertiary email addresses, your primary will still be safe.
- Fifth Level Address–This is a separate address for things like prepaid credit cards that you would use to shop on sites that you don't necessarily trust but may be legitimate and have items or services of interest to you.
- Sixth-Level Address: This is for personal communications not related to financial matters. Use it for family, friends, and others that you routinely communicate with.
- Seventh Level Addresses – use these for social media accounts. Ideally, you should have one for each social media account so that you don't wind up with all of your accounts being targeted if one is breached.
- Seventh Level Address–Use this for anything online from

which you might get newsletters or others that might be spammers or scammers.

Avoid Mail Forwarding

Even though a minimum of seven email addresses may seem like a lot to check, it is very important not to forward these email addresses to one single account. If the catch-all account is hacked, then anyone snooping into it can look at deleted emails or those that arrived since your last login to find out where your other accounts are. This will completely destroy the safety of multiple email addresses.

The other problem with forwarding is the fact that any of your other email addresses can also be hacked. If the hacker looks into your settings, they can easily see where the emails are being sent, and then hack that address.

Watch Your Passwords

When setting up passwords, use a different password for every account. Never use an online document or retrieval source for your passwords. If you need to keep a list, use a handwritten one and keep it secure at all times. If you need to keep several copies of the list, write them all out by hand.

Use at least 12 characters composed of:

- At least 3 capital letters. These capitals should be within words as opposed to just at the beginning of new words in the password sequence. If part of your password is “haven”, then use something like hav3en, or even hav3n.
- At least 2 numbers. Here again, don’t use them as spacers between words. Put them in locations where they break up the text. For example, if a part of your password is is “blanket”, then do something like

bl2anket instead of 2blanket.
- Use the same idea for non-alphanumeric characters. Here again, use at least 2 characters.

I don’t recommend using complete nonsense, as in without some kind of word pattern, because password-breaking programs might hit on it faster as they go through different combinations of numbers and letters.

Hardening Backup Passwords

If there is one thing that makes me cringe, it is the “security questions” that require answers only you would know. The problem with that is ancestry sites and social media posts and comments provide all kinds of information that may be a first or second guess for a hacker. Use the same protocol you use to set up your primary passwords.

What About 2FA?

Even though most websites give you an option for “2-factor authentication”, I’m not necessarily a big fan of it. If your primary device is hacked, then 2FA may not do you much good. You can still set it up and make use of it as you see fit. Just be aware that it isn’t a replacement for robust password structures and layers of email addresses.

The Devices You Use and How to Access Your Emails

You will be best served by choosing just one device to access email accounts and for financial transactions. This way, you can reduce the risk of your device being contaminated if you land on a site with malicious software. Keep this device powered off when not in use.

Here are some other guidelines for using the device itself:

- Install as few apps as possible. Do not install separate apps for each bank, email address, etc. Remember, these all usually come through one installation service. If that gets hacked or compromised, the apps within the store may also be targeted. Instead, use online interfaces as often as possible for logging in.
- Never store password data on the device. Even though it may be annoying to manually re-enter passwords, it is better than losing all that information if the device is hacked.
- Always keep your device up to date and keep up on news related to patches and other problems.
- Always delete emails as soon as you read them, and then empty the trash bin manually. If you need to remember something, write it down by hand.
- Make sure you log into each of your email addresses at least once a week. Keep the information on a handwritten schedule so you don’t forget any of them.
- Always log out of each account manually as soon as you are done looking at the information.

Hardening your email addresses can take some work and create some inconvenience. On the other hand, if you wind up with a hacker that targets you because of something you say online or because you look like you have money, it will be much worse. When you limit the damage that can come through each hack, you

will be well on your way to keeping your financial, personal, and business communications safer in times when people are desperate to take what they can from anyone that they can take it from.