Cover Your Bases: 10 Cybersecurity Basics

You need to protect yourself from all of the threats that exist in today's world – from hackers to scammers and malicious actors to ransomware and other malware. **It's hard to know what to do and where to start.**

The following list focuses on the most powerful security YOU can implement today to protect your data, privacy and online security:

1. Share with care

Share with care and be mindful about what you share on social media. **Social medial is the launchpad of all successful Social Engineering attacks and hacks.** Protect your personal and private information and share information only with those you trust. On Facebook (and other services like LinkedIn), review your privacy settings and the privacy settings of everything you have posted. Time spent here will decrease the chances of a hack or scam. (Hueya software does this for you!)

2. Protect your data

Backup, Backup, Backup. Backing up your computer is your first line of defense against a disaster – backup your computer and any devices daily. Backup to a solid state external drive daily and when finished, disconnect the drive for safe keeping. By disconnecting your backup drive, you further protect your data from an attack if you get hacked.

3. Update your software

Apple, Windows and Android release security updates and fixes (patches) on a regular basis. Don't become the next Equifax – apply software updates on a regular basis. This includes your operating system (Windows, OSX, Android, Apple iOS) and all applications (Quickbooks, MS Office, Dropbox, Slack).

4. Email Scams

Distrust but verify. It can be tough to distinguish between emails that are legit and those that are not (phishing emails). Our rule is to distrust the communication until you can verify whether it's a scam or not. Another indicator that the email is a scam is that it asks you to do something – don't fall for it. If the IRS is after you – you will know. Until then, ignore and delete. Pickup the phone and call the institution that sent the email and/or search google to see if it is in fact a scam.

5. Phone Scams

Again, **distrust but verify.** Scammers and social engineers use public data about you to their advantage and they sound very legit. Hangup and call the institution back at a verified phone number. Also, Microsoft or Apple will not call you directly out of the blue – and if it appears they are – you now know what to do.

6. Passwords and Password Hints

Use passwords you can remember and do not use anything in your password (or password hints) that you might have shared on social media. This is why we share with care – see above^^! When choosing a password, use a sentence that is easy to remember. Here is an example: 'Ocean heffer swimm!ng upstr8am.' Also, check to make sure that your accounts are not hacked and change your passwords every couple of months.

7. Multi-factor authentication

Multi-factor authentication adds an **additional layer of account security** to your login process that hackers do not have access to. This is often something that only you know or have and is required to login to your account. Multi-factor authentication is offered by most mainstream companies and is an excellent control to enable.

8. Protecting your utilities so they protect you

Setup phone passwords with your bank and financial institutions, mobile carrier (Verizon, ATT), internet service provider, phone company, power and water. You will need to call each one of these companies and manually setup this additional layer of security. By doing this, you are disabling the ability of a social engineer (hacker) to circumvent your security controls (multi-factor authentication).

9. Credit Monitoring

In light of recent events (Equifax), monitoring your credit has never been more important. Credit monitoring enables you to see in real time if someone is attempting to take financial advantage of you or your family. If you have not frozen your credit – go ahead and do that as an added layer of protection.

10. Hack Yourself

Type your name in Google to see what comes up, you may be surprised what you find. Opt out of all of these services by finding their opt-out page. To do this, do not search yourself by using the service, rather type in google 'peoplefinder opt-out' – this will save you alot of time and a big headache. Some of these services are hard to opt-out of because the information they are sharing is being exposed by your local county property database. Contact you local officials to protect access to this data.