Praxonomy Blog
EMPOWERING BOARDS

Digital Hygiene for the Board

Written by Jay Shaw on January 29, 2019

There is no such thing as 100 percent digital safety but by learning good practices and taking simple steps to protect yourself, you can make it much harder for anyone to hack into your computer or eavesdrop on your phone calls or online communications.

According to a report from an expert group working with Germany's Federal Crime Office, a third of small and medium businesses have already been hacked. You can read the report here:

Germany: Third of small and mid-sized companies have been hacked

What's true in Germany is likely to be true everywhere, which suggests that it is just about guaranteed that either you and your fellow board members have already been hacked or that you will be targeted soon.

So, if you haven't started already, you should start thinking about how you do what you do online. This does not mean that you need to become a digital security expert. Rather, it means that you should take reasonable steps to keep safe.

Here is a list of suggestions, each of which is easy and quick (and in many cases free):

Encrypt your hard drive (and back it up locally while you're at it)

If you're using an Apple computer, the built-in drive encryption option is called FileVault. It takes a little while to spin up the first time but once it's done, your computer is very, very hard for just about anyone to crack. The Windows equivalent is Bitlocker.

Activating drive encryption costs nothing and will keep your data safe should you ever lose (or temporarily lose physical control of) your computer. It's well worth doing. While you're at it, turn on the built-in firewall option, which will not limit your Internet use in any way but will keep stray programs from reporting out and from downloading who knows what in the background.

Both Windows and macOS support automatic back-ups. Buy yourself a large-capacity portable hard drive (they're cheap as bread these days), plug it in and let the back-up software do its thing. This way, if you are hacked, you can back down from the last clean back-up and consider yourself lucky to have dodged a bullet.

Get an anti-virus program and turn it on

I use ClamXAV for my Mac. It acts like a sentinel for incoming data. Once in a while I set it to scan everything and just let it run all night. Over the years it has found and disabled quite a few viruses, mostly viruses that people have unknowingly sent me via email.

Windows 10 comes with Windows Defender built in, which, according to reviews, isn't a bad antivirus solution. Some friends and colleagues use it alone. Others use it along with an anti-malware program. Yet other people use third-party solutions for everything. Almost anything is better than nothing so choose something and make sure it's installed and working.

Anti-virus applications are less common for mobile operating systems because mobile systems are generally better protected against viruses and malware than desktop systems. In general, iOS is thought to do a better job against viruses and malware than Android. That said, no system is perfect. You should be very careful when choosing which apps to download regardless of operating system. Review your app "portfolio" regularly and delete any apps you no longer use. And don't click on anything sent to your phone via SMS, iMessage or email from an unknown party.

Also, make sure you turn on auto-update for your operating systems as well as for your phones and apps so that you always have the latest security patches installed.

Get and use a password manager (and go for 2FA where you can)

I used to know passwords. No more. Now I use Padlock, an open-source solution, and let it generate random 10- to 20-character passwords for each of the more than 60 services I login to on a regular basis. I have Padlock on my laptop, on my phone and in the cloud. All three are set to synchronize on launch, in effect serving as back-ups for each other. I also export everything in plain text to a USB drive once or twice a year and put the USB drive in my safety deposit box at the bank. This way, if I die my family and colleagues can still access the business and other services for which I am (or will have been) responsible.

Along with making compulsive use of a good password manager, you should opt for two-factor authentication (2FA) wherever you can. You can use a stand-alone device like Nitrokey or YubiKey, a software application like Authy or Google Authenticator or have the service message a one-time-use code (usually a six-digit number) to your phone or email whenever you login. However you do it, a two-factor solution will always be more secure than single-factor authentication.

Companies that have gone 2FA have cut credentialing hacks by impressive margins. Google gave a Yubikey to every employee to stop phishing attacks. It literally cut the incidence to zero. These device keys are not expensive and they can be used with laptops, tablets and smartphones.

Both Microsoft and Apple are looking to "no password" credentialing solutions. But switching channels by itself may not be orders of magnitude better than current single factor authentication. A code sent to your smartphone is good but would be much better if it were paired with a strong password. Of course biometrics such as fingerprints and Face ID can serve as powerful authentication components too. But for critical files and services you may want to at least pair biometrics with something else.

Last week at dinner my 15-year-old daughter logged on to her 13-year-old sister's iPhone with Face ID. A classmate's mother can do the same with her daughter's iPhone. Apple says that Face ID technology is not "twin safe" but neither my daughters nor their friend and her mother are identical matches – not by any stretch of the imagination. It's not just face recognition that needs more work. Fingerprint recognition has been cracked, as have voiceprints. The bottom line is that no biometric recognition framework is foolproof. 2FA is the smart move.

In fact, a very-high-security authentication framework would make use of at least three things: something you know, something you have and something you are – for example, a password, a physical key of some kind (or a code sent to your smartphone or sent via email or else generated by a stand-alone software application), along with a voiceprint, fingerprint or Face ID.

Buy a VPN service subscription and use it

A Virtual Private Network (VPN) sends your digital communications via secure tunnel to a server which then anonymizes your requests and sends them on to the services you want to access. The target services will still be able to profile you (to some extent) but nobody looking for you on the network can see what websites, email servers or other online services you're accessing. This is powerful data privacy protection and a must-have for all of your devices.

There are many good VPN services. They are all pretty cheap and the sector is well reviewed so you have your choice of provider. I use ProtonVPN, not because it's the best, though it certainly is one of the best, but rather because ProtonVPN

is a sister company to ProtonMail, and I can use both services with one subscription. Torguard also offers both VPN and secure email services.

Have the board get on a separate, high-security email program or use PGP (or both)

Here at Praxonomy we use Kolab Now, a great email and general business collaboration tools service. Note however that even highly secure email services are still susceptible to some data leakage, not the content of individual emails so much as information about who sent the email to whom, when it was sent and whether or not the email contained attachments. This is "heading metadata" and is quite difficult to hide. But as long as you're not a global celebrity, high government official, journalist or human rights activist looking to hide absolutely everything, even your metadata, a secure email service will more than suffice to protect your sensitive content. People in very high-risk classes can use yet other options, like dark-web email services, but those options fall outside the scope of this discussion.

Keep in mind that it's easy enough to create a new domain name such as www.board-yourcompanyname.com and point the domain to your new email service so that you end up with email addresses that look like firstname.lastname@board-yourcompanyname.com, that is to say, like normal corporate email addresses.

You might also consider installing GPG Suite on your Mac or one of the Windows equivalents such as Gpg4win on your PC to encrypt the content of your emails. Get the whole board to do it. With email content encryption, even if you cannot move to a separate email service, you can still protect the body content of your email conversations so that prying eyes cannot see what the board is discussing.

Use a high-security messaging application

Whatever mass-market messaging application you're using now, stop and replace it with one of the high-security messaging applications. There are several options, some at no or low cost, and they are good.
Telegram is a Dubai-based service founded by expatriate Russians. It has millions of users around the world. One of my colleagues tells me that it is the best general messaging service he has ever used. The Russian government keeps trying to shut it down so the Telegram team must be doing something right.

Wickr has a great reputation among corporates, as does Silent Circle. At Praxonomy we use Wire, which is absolutely excellent. We are big, big fans. At home I use Wire when I need to screen-share or do video calls and Signal for plain old texting and voice calls. Signal is a beautiful, easy-to-use application that reportedly made one senior computer scientist cry when he saw just how elegant the code is (it's open source, as are Wire, Wickr and Silent Phone – Telegram is not open source but does have an open API).

Use one of these messaging services. There is no good reason not to.

Harden your browser

As for browsers, Chrome sends a great deal of information straight back to Google. According to a recent article by The New York Times, Chrome on Android sends your location details back to Google up to 300 times a day. Safari is a bit stiff in regard to set-up options. Firefox is just about right but even Firefox needs to be set up properly. Look carefully at the privacy settings. There are always trade-offs between safety and ease of use. Don't be afraid to experiment. You may want to use a "no track" search engine like Duck Duck Go instead of Google or Bing. You may want to clear cookies and history on logoff. Keep trying the set-up options until you get to what you need.

There are other browsers, both chromium- and Firefox-based, with more privacy controls, Pale Moon, Waterfox and Brave being some of the better known options. Microsoft recently announced that the new Microsoft Edge will be chromium-based. This will likely work well without automatic data sharing with Google, which can only be a good thing.

Choose a cloud storage service with serious, end-to-end encryption

Tresorit is a truly impressive, end-to-end-encrypted cloud storage and sharing application. We recommend it for board use. What we don't recommend is use of unencrypted or partly-encrypted mass-market cloud storage applications, even if they are free.

Even if you don't use a service like Tresorit, you should consider encrypting sensitive board files before attaching them to emails. PDFs can be encrypted, as can Microsoft Office, Open Office and Libre Office documents. Many people do not know that password-protected encryption is an option for common file types. Try it. It's not so hard to do.

Consider one-to-one encryption for important documents and files

Another possibility is to use applications like GPG Suite's Services options (control-click while selecting the document), which provide military-grade encryption for documents and files on a public / private key basis, meaning that only selected recipients can decrypt the file.

Use common sense and, of course, think about using a board portal *(hey, ours is pretty good)*

There is a whole world of ultra-high-end protection that the law-abiding, very careful user can adopt: the Tor Browser and Network, Tails, Haven, Veracrypt – the list goes on. But these options are steps too far for most of us. The recommendations above are more than enough for most board members (and most other people too).

Keep in mind that the single best move you can make to keep out of harm's way is to exercise care. An attitude of healthy skepticism goes a long way when it comes to keeping yourself safe. Don't visit dodgy websites. Don't click on attachments or URLs in emails from people you don't know. Even if you do know the sender check the extended heading information. Any bad actor can append a familiar name to a sketchy email address. Don't assume that the voice on the phone is the person the voice claims to be. Don't click on phone message icons or URLs from strangers. In short, don't make yourself an easy target.

By being careful and taking some simple, easy steps you can make yourself and your board much harder targets to hack.

And of course your next best move would be to take a good look at secure board portal options. The Praxonomy board portal is well worth considering and we would love to talk to you. Give us a call or sign up for a free trial here.

ABOUT THE AUTHOR

Jay Shaw is the Founder and Chairman of Praxonomy. Jay is a serial entrepreneur with over 20 years experience in the IT industry. Prior to founding Praxonomy, he was the Co-founder and CEO of NetDimensions, a London Stock Exchange AIM listed enterprise software company. Jay also serves as the Non-executive Chairman of SandSIV Group, a software and services company based in Zurich, Switzerland.