Security & Privacy Best Practices

Below you will find key concepts and resources from our recent cyber-security training session. In the bottom section you will find links to guides and checklists which may be of use both personally and professionally. Remember, this is a weakest-link scenario. We want to not only protect ourselves, but also protect colleagues, family, and friends because often hackers will target people in our lives in order to find a path into our data and infrastructure. You are welcome and encouraged to share these resources with colleagues and family, but please do not post these links on social media or the internet as we would like to protect the trade-craft. Hackers are constantly monitoring our tactics and working to counter them in their cyber-attacks.

Ransomware Key Concepts

- Phishing is the #1 point of entry for ransomware attacks. Awareness training and teaching staff to avoid clicking on suspicious links or attachments in emails will drastically reduce the risk of a successful ransomware attack.
- Prevention will reduce the chances of a successful attack, but still we should prepare to get hit.
- Make an incident response plan, assigning roles and responsibilities for the first 12 hours of the attack. Your IT manager or IT vendor should be able to assist you in developing that short term plan. Make sure to address what you will use for communications if company email is compromised.
- Identify a Law Enforcement team that you will notify should you be attacked. In most major cities there is an FBI cyber task force. They may not be hugely helpful depending on the scale of the attack, but notification of law-enforcement should be part of your post incident due diligence.
- Understand your cyber insurance policy. Does it have coverage for incident response support?
- Prior to facing an incident have discussions regarding your stance of paying the ransom if things become dire.
- Do you have resources to help you negotiate and pay in cryptocurrency? If your insurance policy does not cover these things, research potential vendors to assist with the help of your IT manager or vendor.
- Understand that if you pay it may subject you to future attacks and you may get bad press for doing so.
- How often are your backups tested to ensure that they will function properly if you choose not to pay?
- If you don't pay, the hackers will likely threaten to leak stolen client data so have a plan to notify impacted customers, vendors, etc. Do some research up front on your state laws regarding breach disclosure deadlines or discuss with your legal counsel.
- The most important thing is to have a plan and that key personnel know the plan and have access to documentation (outside of the network resource as those may be compromised). Hard copies of your incident response plan are recommended.
- Run a two-hour table-top exercise wherein key managers and personnel talk through post incident steps and responsibilities.

Breach Data – Actionable Steps

We all have personal and professional data contained in third party breach data. Hackers buy, sell, and trade these data sets to use against us in phishing and other cyber-attacks.

- You can check to see which breaches have your data in them by querying your email addresses at the following vetted security site: https://haveibeenpwned.com/
- You can also set up notifications on future exposures at https://haveibeenpwned.com/NotifyMe
- Once you identify personal email addresses that are exposed, use your password manager (**see the training resources below for password management recommendations and steps)** to log into affected accounts and set new long, unique passphrases. A passphrase is just a password that includes several words so that it is much longer and harder to crack. Your password manager will auto-generate these for you.
- Haveibeenpwned.com is a vetted third party organization which you can use to search for exposed company emails. They will also provide breach notification for future exposures, but they first have to verify that you own the domain for which you are requesting data. The easiest way to set this up is to have your IT manager or whoever runs you web-site request the service. You or your IT manager can set up breach notification for your company domain (web-site) at: https://haveibeenpwned.com/DomainSearch
- Any corporate emails that show up in breach data, have IT lock that account and prompt the end user to set up a new, long, unique passphrase. Supplying employees with password managers will encourage them to use good digital hygiene. Password manager recommendations are available in our training resources.

Training Resources

Our training site IntelTechniques.com has many resources that are targeted towards our clients who are in a much higher threat-model such as military, law-enforcement, etc. You are welcome to look through any of our content, but you do not need to buy anything and please understand that the podcast, blog posts, and books contain measures that are likely more extreme than you require. Below are the free resources that are likely most pertinent you, your organization, and your loved ones:

- Presentation Resource Page (this includes links to our recommended password managers and other privacy/security respecting services): https://inteltechniques.com/links.html
- Privacy/Security Packet: https://inteltechniques.com/data/je/privacy.pdf
- 10-Day Security Guide (this is a set of basic, achievable steps for those new to privacy/security): https://inteltechniques.com/data/je/SecurityEssentials10DayGuide.pdf
- Credit Freeze Guide (the most effective measure to prevent identity theft): https://inteltechniques.com/freeze.html
- Remember, your number one resource is listening to your own instincts. If something feels wrong it probably is. Make certain employees know who in the organization to notify if they see something suspicious.