You've Completed the Security Quiz!

What now? Go to your score section to see our advice!

Scores of 1-5:

Uh Oh! You're in need of some help!

Our advice? Seek out a network scan from a reputable company, get a good antivirus, and invest in some anti-phishing software and a password manager. And get some official business emails!

Multi-Factor Authentication (also known as Two-Factor Authentication) will protect your business from the *vast* majority of password brute-force attacks and buys you some time to change your passwords in case of a breach. And, if you know your employees reuse their passwords but you can't fix that right away, enabling 2FA on the big accounts (like email and Microsoft accounts) will provide more protection while you get that fixed!

Email: employees *should* have separate work and personal email accounts! If employees frequently use non-work accounts to discuss work-related matters, it makes it much easier for a phisher to use a social engineering attack to get into your network or steal data directly from the employee, impersonating someone else! Business emails are harder to impersonate.

Wi-Fi, if it applied: your Wi-Fi should always be secured! Guest Wi-Fi should be separate from the Wi-Fi you do your important business on, and in any case, Wi-Fi should be password protected. Scammers can get into any data transferred over Wi-Fi if they can just plug right in!

Scores of 6-10:

Good, but could be better!

Our advice? Spend some time fine-tuning the settings on your systems! If you have antivirus, but turned it off because it was getting in the way too often, revisit those settings or go to a different vendor. It's not worth getting ransomware!

If you skimmed the 1-5 section above, you probably see how important a safe, secure, business-only email with a good password and MFA (multi-factor authentication) to protect it is. If you're certain your network doesn't have any open ports, and your antivirus is active on your computers, your next biggest threat comes from email, whether that be phishing or account hacking.

Make sure your employees are well-trained on what phishing is, how and where it's okay to store their passwords, and how to spot social engineering attacks before they turn into network-downers.

Scores of 11-15:

Well Done!

Our advice? Keep it steady! Strong passwords, 2FA, and protected WiFi make getting into your network much harder. Maintenance, such as keeping programs and operating systems up to date, will continue to provide protection. Microsoft frequently updates to keep itself secure and free of vulnerabilities, so when it offers an update, take it!

Some simple stats for you, the Business Owner

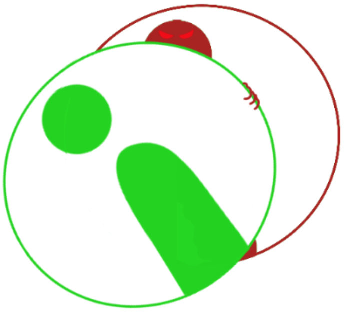
So why do we recommend the things that we do?

2FA prevents a whopping *95%* of brute force password attacks on email accounts.

2FA (2-factor authentication, also known as MFA, or multi-factor authentication) is the easiest way to increase your password security and turns a stolen password from a pants-on-fire emergency into a simple, easy fix.

Phishing can compromise an entire network.

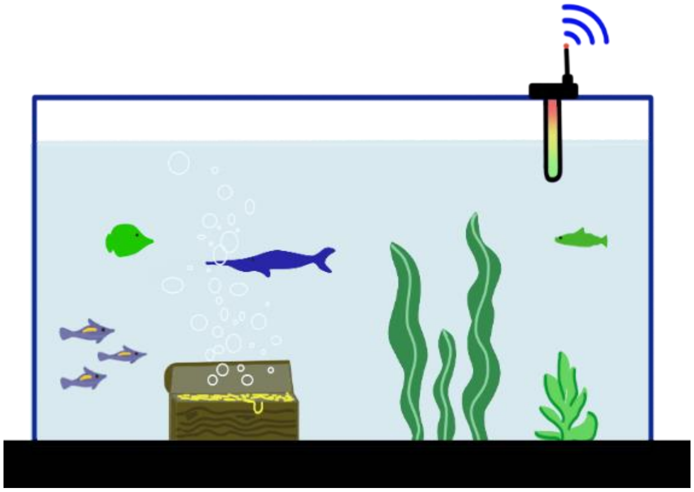
Not all phishing is easy to spot! Spearphishing is a type of phishing that deep-dives into available information to make a convincing fake. Social media profiles and information available on the official website can provide a determined hacker with everything they need to fool a coworker into handing over valuable information or trying to log on to a fake page for a real website.



While your employees might be able to spot a bad phishing attempt with no training, would they be able to spot a pretty good one?

So can poorly secured Wi-Fi!

Wi-Fi is tough, but you can still do a lot to secure it! Firstly, use passwords to protect your network, and don't let strangers join it. An unsecured Wi-Fi network like the kind you find in coffee shops is an easy target for hackers, who can steal data transferred over Wi-Fi with a little technical know-how. Even if your company is providing the WiFi, without a password, it may as well be that coffee shop.



IoT items are problems waiting to happen.

Internet-of-Things items (sometimes just called IoT) are anything Wi-Fi connected that's not 'traditional' office equipment like doorbells, coffee makers, robotic vacuums, etc. and should be kept off your network *or* given a password.

A casino was hacked because their fish tank's thermometer was connected to their network! (Story here: https://www.entrepreneur.com/article/368943) Open ports anywhere in your network can pose a risk, but IoT are the easiest to get rid of. You don't have to throw it away, just keep it off the network!