Checklist: How to Avoid Becoming a Victim of Cybercrime

The Problem

Over the last 13 years, I've seen certain attacks happen over and over again. The good news is that there are some simple steps to protecting yourself from becoming a victim of these attacks. I will share these steps with you below.

Note: If you need help with any of these items we are here to assist you.

The Checklist.

- Utilize a skilled cybersecurity firm to assist you in developing your plans and policies.
- Enforce that all wire transfers have a multi-step verification process. This will help you avoid unwanted wire transfers from happening. (I received a call once where cybercriminals were able to wire $500,000 out of a companies bank account to their own account offshore. The money was not recovered.)
- Encrypt your emails and text messages. This will help prevent unwanted eyes from access your sensitive data.
- Know your attack surface. Keep an up to date inventory of all the devices in your attack surface.
- Setup email filtering to cut up to 80% of phishing emails from hitting your organization's inbox.
- Backup your data frequently to an off-site location and break the connection to the back up after the backups are complete. Test your organization's ability to recover from your backups to get back up and running.
- Have professionals test your networks, web applications, email systems, etc. to see if/how they can break-in then have this firm show you how to repair your weaknesses.

(Penetration testing) You can only protect yourself if you first know how the bad guys are going to attack you.

- Enforce multi-factor/two-factor authentication for all log in procedures. (Even if a criminal has your password they cannot successfully login without the multi-factor authentication code.) This is where you have to receive an extra code/step before you can log in even if you have the correct username and password. **Note:** This is one of the most important things you can do today to protect your organization.
- Implement security awareness training & tools for your staff *(This will help reduce your susceptibility to phishing attacks.) This training teaches you how cybercriminals attack and how to avoid becoming a victim of their methods.*
- Control what devices can and cannot be used in your organization.
- Keep your antivirus/anti-malware up to date.
- Utilize a VPN (Virtual Private Network) for all work-related internet access needs.
- Establish a clear security response plan for when an attack does happen. Test this plan often.
- Implement reputable firewall/intrustion detection/intrusion prevention tools.
- Monitor your organization for unusual access, activity, and data exfiltration.
- Utilize a cyber insurance policy.
- Instill a cybersecurity mindset in your organization. Make it part of doing business, part of your culture. You and your people are often your first line of defense.
- Create and enforce strong password policies. (Do not reuse passwords across accounts. Remember, multifactor authentication must also be set up.)
- Install reputable antivirus software and keep it up to date.
- Keep your software patches up to date (Equifax suffered a breach from not patching properly.)
- Avoid public WIFI. Use your mobile phone cellular data to connect to sensitive accounts when working out of the office. WIFI. is often not as secure as your cellular data connection. **Note:** Nothing is 100% secure.

Conclusion

This checklist will help you better protect yourself from the most common malicious attacks.

If you have further questions please don't hesitate to reach out. (Contact info below.)

In your service,

Jeremiah Baker

Cyber Security Speaker & Consultant

617-872-2875

jbaker@jeremiahbaker.com