CORE SECURITY

How to Build a Culture of Security

March 2016

Table of Contents

You are the target.

Gone are the days where robbers run out of a bank with bags of money or someone sneaks in at night and steals your proprietary information.

The hackers are no longer going after the company, they are going after you. With your credentials, they can slide into your organization and take information without anyone noticing.

This means you are the target and any data you touch, from your user credentials to network tokens, you are ultimately responsible for keeping safe.

Here are 10 things to look out for and recommendations for how to keep all of your information safe.

Social Engineering

Social engineering hacks consist of a very sophisticated approach where the hacker pretends to be someone you know or trust - such as your bank or even a friend or co-worker - and will use information he gains from social networks to win your trust.

While these attacks generally come in the form of an email, they can be delivered by instant messaging, text messages, or even in-person attacks.

Train your teams:

- To look for common indicators such as people asking for information they shouldn't have access to, using a lot of confusing or technical terms, creating a sense of urgency, or the general "if it seems too good to be true, it probably is."

Phishing and Spear-Phishing

Phishing attacks are skyrocketing along with the more targeted "spear phishing" attacks.

These attacks use the information gained through social engineering to gain your trust and are trying to get you to do something seemingly harmless such as click on a link or open an attachment.

Train your teams :

- Just because a message seems like it comes from a friend doesn't mean it is safe. Hackers could have taken over a friend's computer or account or simply spoofed the "from" address.
- Be suspicious of any emails directed "Dear Customer" or other generic greetings.
- Be skeptical of any message requiring 'Immediate action' or creates a sense of urgency.
- Be suspicious of any emails coming from an official organization or business that have bad grammar or spelling mistakes.
- Before you click on a link, hover your mouse over it and the true destination will display; confirm that the address is what you think it is.
- Be careful with attachments, and only open ones you were expecting.
- Always treat suspicious emails with a healthy dose of skepticism and common sense.

Browsing the Internet

Internet browsers are one of the easiest ways to get into your computer.

Common techniques are to place hacks on websites you might visit and then launch multiple attacks while you are on the site.

Train your teams:

- If your browser or plugins are outdated, then you are at risk. Always upgrade to the most recent versions.
- If your browser warns you not to go somewhere: Listen! Or contact your IT department for more information.
- Do not install plugins or add-ons unless you absolutely need them and they are approved by your IT department.
- Be sure your connection is encrypted whenever you connect to sensitive websites. Not sure if it is safe? Look for "HTIPS" on the website address.
- Always scan any files you download with anti-virus software.

Social Networking

Social networks are the new watercooler, and we don't expect anyone to stay off of them while at work. However, all social networks should be used securely.

Train your teams:

- Social networks are phishing's number one tool; don't give out any information on these sites unless you're ok with the world knowing it. Be weary of any messages that could fall under the "phishing" guidelines.
- Be careful what you post; your information could be used to steal your identity, guess your passwords (what year did you graduate?) and commit online fraud.
- Be careful when integrating third-party websites with your social network. Not all security is the same. Just because you don't mind Facebook linking to your home computer doesn't mean it's ok to link them to your company computer.
- Only access social networks from work devices IF approved by your IT department.
- Never share sensitive information.

Bringing Your Own Device (BYOD)

Just like with social networking, it is becoming impossible to keep employee devices off of your network. To make sure that none of these devices are impacting your network, make sure to put a BYOD policy in place that includes the following:

- Differentiated networks: Only approved networks can be reached by employee devices so that your most sensitive data can stay safe on its own network.
- Only install apps that you need and only from trusted sources. Always update them when available to keep highest security.
- Disable Bluetooth when you are not using it and Wi-Fi
- Do not access or store work email or other data unless you have been authorized and have proper security in place.
- Protect your devices with hard-to-guess PIN numbers and encrypt your data if that is an option.
- Consider enabling remote wiping.

Passwords

With the surge in online applications, users have multiple accounts with credentials . In order to keep that access safe, they need to make their passwords not only differentiated but also hard to guess. Here are a few more ways to keep your passwords secure.

- Use a passphrase instead of a password.
- Require a number and/or a symbol in your passphrase.
- Have at least one upper and one lower case letter.
- Use Multi-Factor Authentication - that is, using a password and a pin or a thumbprint and a password.
- Make it a policy to change login credentials every 90 days.
- Use different passwords for different accounts.
- Never share oasswords with anvone. even your supervisor. Do not use public computers to log onto work or bank accounts with your password.
- Be careful of websites that ask you for personal questions. Only use personal questions that no one else can answer (remember social engineering).

Encryption

Encryption is a process that makes your information unreadable or unusable to anyone who doesn't have the key to unlock it using algorithms to construct a unique key to encrypt and unencrypt your data.

All data should be encrypted going both ways for ultimate protection.

Examples of things that should be encrypted:

- Laptop, mobile phone, USB sticks - anything that is mobile or can leave the premises
- Communication protocols - VOiP, instant messaging, email
- Electronic files and folders
- Browser connections to websites such as online banking, social networking, online shopping

Data Retention

We live in a world of big data with more and more information being shared and stored each day. But what do we really need to store? The answer is: only what you absolutely need.

Here are a few other tips for data retention:

- Only use systems approved by the organization to store or transmit data and never store data on personal laptops, phones, or other devices.
- Do not transfer data without encryption .
- Do not store sensitive data without encryption and never store or share sensitive information on public internet or cloud services.
- Never leave sensitive documents open at your desk and always lock your computer.
- Use only authorized software for work-related activities.
- Any third-party vendor provided with data needs to follow the same security protocols. This may require a contract.
- Any sensitive information that is no longer necessary or appropriate to store should be properly destroyed, shredded or rendered unreadable.
- If you believe data has been lost, stolen, or compromised, contact your security team immediately.

Wi-Fi Security

Everything you do over Wi-Fi - even on networks requiring passwords/log-in information - can be monitored.

Not only can everything you say, type, or send be monitored, but hackers can use your connection to penetrate your network and compromise your computer or online account.

When you are connected to any Wi-Fi network, make sure that all of your communications are encrypted, especially on public Wi-Fi networks.

If you have Virtual Private Network (VPN) capabilities, utilize it when using public Wi-Fi as it will create an encrypted tunnel and will allow you to work more securely.

Insider Threats

Outside attacks are not the only threat to your organization. People inside - employees, contractors, and third-party vendors can also cause you harm.

The insider has both physical and digital access to your systems.

Look out for:

- Someone carrying a large number of documents or downloading extremely large files for projects they are not working on.
- Someone working strange hours or working when others are off the clock.
- Someone trying to log on to others accounts or get access to systems or applications they shouldn't need.
- Someone changes their behavior drastically.

In order to minimize insider threat:

- Only give people access to the applications, data, etc. that they are responsible for as part of their job functions.
- Store sensitive information in appropriate locations.
- Always lock your computer and desk when you are away for any period of time.
- Never share your password or credentials with anyone - not even your supervisor.

Working Remotely

Between our laptops, tablets, and cell phones, we are constantly working. While this is good for us and our business, it is also good for hackers who have increased entry points into your system.

- When working remotely, make sure you only use devices that are authorized by your company or that are covered under your BYOD policy.
- Keep your devices physically secure at all times; stolen laptops were a huge percentage of health-care data breaches last year.
- Always use VPN when on public networks and that all applications are using encryption.
- Never use a public computer for work; you do not know if they are secured properly.
- Always password-lock your computer when you leave it and do not allow others to connect devices to your laptop.

How Secure is Your Culture?

How many of these policies do you think your employees already follow? How many do you think they need to follow? Unfortunately, every organization's number one resource is also their number one threat- their people. By building a culture of security in your organization, you will help build a secure network from the inside out.