A quick guide to

SAFE WEB NAVIGATION

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

See what your technology can do.

www.visualedgeit.com

Introduction

Looking at the growth of cloud computing and the available access to business systems from anywhere at any time, it's easy to see how our dependence on the internet at home and work has only continued to grow. The number one concern for companies is security because cyber attacks are happening at a record pace... in fact some research claims that there's a cyber attack attempted every *11 seconds*.

But that's not the scariest part: cyber criminals are only getting smarter with their approach. They are continuously developing new and advanced techniques to break through all types of security measures, and according to Statista, cyber attacks are one of the fastest-growing types of crime in the US.

In order to secure their network, business systems, and data, many companies get assistance from managed security service providers (MSPs) to keep their data and systems safe, put multiple backups in place, and create backup and disaster recovery plans for worst-case scenarios.

Businesses, both large and small, are always at risk of cyber attacks though because of the human factor. Without an awareness of the different ways that cyber criminals gain access to a company's network, employees' online browsing will always be a liability for a company. Small businesses especially are more vulnerable to cyber attacks because their security standards may not be as high as larger companies. Cyber criminals know this and will target unsuspecting employees through different tactics.

Minimizing company risks of employees browsing the internet starts with understanding the risks.

Understanding the Web of Risks

Having employees understand the risks of careless behavior online helps instill good online behavior and minimizes the chances of a cyber attack or data breach. Below are the most common types of cyber attacks that companies experience.

Malware Attacks

Malware, short for "malicious software," creates significant damage to a computer, server, client, or network. Cyber criminals typically use this type of software to extract data and either hold it hostage or sell it on the dark web. These are the most common types of malware:

- **Ransomware:** You know those movies where a kidnapper holds a hostage up in a bank or the back of a windowless van until a ransom is paid in exchange for their release? This type of attack works exactly the same way, except it's your critical data that's held hostage until the ransom is paid. Ransomware attacks are on the rise, and often the criminals will threaten to publish sensitive company data or information if the demands are not met. They encrypt the data and make it unusable for you until the ransom is paid.

- **Spyware:** This is used to track internet usage data and other personal information, such as online bank account information, credit card information, and additional personal or financial information. Criminals capture this information and then sell it to advertisers, data firms, and other criminals.

- **Adware:** This has become so common that we probably don't recognize it as dangerous anymore. Having adware on your computers will trigger pop-ups on your computer screen when you browse through unknown websites. It gains access to your computer via toolbars or browser extensions, bundled software, and downloads offered by pop-ups.

- **Computer Virus:** A form of self-spreading malware that replicates itself by modifying other programs on a computer. These can gradually spread to other computers in the same network and cause severe damage within an organization.

Social Engineering Attacks

These types of attacks use manipulation to trick people into providing sensitive information associated with their personal or financial data.

- **Phishing:** This is a specific kind of social engineering where you may receive an email, phone call, or even a text from a seemingly trustworthy source. You may be required to click on a link and then get redirected to a website requesting personal or financial information, or the link may be a trap to install malware into your system.

- **Spear phishing:** This is a highly targeted type of phishing attack where the attacker focuses on a specific individual and uses personal information obtained from social media or other online activity to get financial data or company information.

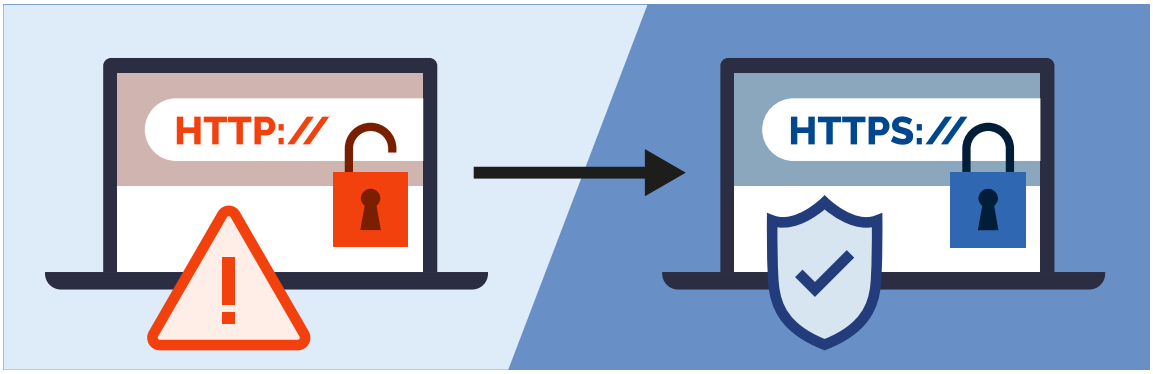
Understanding the Warning Signs

While this guide has highlighted major threats that target online activity, your employees may still end up on a malicious site without knowing. It's a critical part of a business' security efforts to educate and train employees to identify safe websites and potential threats that can lead to malicious websites.

Signs of a secure website

- **Look for the 'S':** Most sites use HTTPS, which means an SSL certificate protects it. The 'S' stands for secure, which means it's safe to enter personal information because the data is encrypted before landing on the server. If the 'S' is missing, avoid entering personal or financial information on the website because it could be compromised later.

- **Lock icon:** The lock icon appears on every browser and can be found somewhere in the window. Clicking on the lock icon will allow you to verify the trustworthiness of the website. Before entering personal information, read the detailed information under the lock.



Signs of potential threats

- **Email Links:** Never click on links in emails. There are a couple of ways to check the legitimacy of the link:
  - Right-click and select ”Properties” – This will show you the link’s destination.
  - Hover over your cursor over the link to see if it matches the text that appears... Whatever you do, always click with caution!

- **Browser Extensions:** Browser extensions seem harmless—but they’re not! Extensions have access to everything you do online, which means your passwords, browsing history, credit card, and bank account information. They often require that you allow access to read or change everything on web pages you visit.

- **Fake Websites:** It can be challenging to tell a legitimate website from a fake one, but the difference will be in the spelling and accuracy of the URL. The URL may be a variation of the website name but closely matching, so it may not be easy to notice if you’re not looking for it.

- **Spelling and Design:** Misspellings, poor grammar, and inconsistent formatting are a sure sign that emails or websites are potential traps.

- **Attachments:** Files attached to emails from a large company that appears to be one that you most likely engage with can be very damaging. Criminals will send emails from fakes resembling Amazon, Microsoft, or the USPS with an attached receipt or product order. Cyber criminals will attach a sense of urgency to an email, and all it takes is one click to create a big problem.

Encouraging Safe Browsing Practices Across the Organization

When you understand how important it is to follow best practices for internet browsing and how detrimental it can be to a company if an employee doesn't take precautions, it becomes your responsibility to protect the business. Provide information and tools to employees so they can know what to watch for and use safe browsing practices, including:

1. Using a Secure Browser

It is not advisable to use any and every browser. Some companies go so far as to designate specific browsers that employees can use. This ensures that employees use the safest and most common browsers built that emphasizes privacy and security over functionality.

Keeping browsers updated with the newest version provides new features and the latest security patches. You can manage security settings on the browsers that you use, buton't rely on the default settings because they are the basic settings that work with all systems and most likely the least amount of protection. Make sure that you are in control of what security measures are in place.

2. Using a Password Manager

Everyone tends to keep passwords that they can remember... but that doesn't mean that passwords should be as easy for others to guess. Employees use multiple platforms and may be required to have numerous unique passwords. For this reason, people begin using the same passwords everywhere because it's easy to remember.

Providing employees with a password manager allows them to remember just one password while keeping passwords for all other accounts safely secured within the password manager's vault. Even if the organization has a Single Sign-On (SSO) in place, a password manager can fill the gaps. Both tools work best when used together. Simple and workable!

3. Disabling Autofill

Keeping a password manager bypasses the need to auto-fill passwords on the browsers directly. Websites can use hidden fields to steal data from forms. In the event of a system hack, an autofill allows the free pass to the hackers. You may be risking all your personal and financial data allowing auto-fills. Turn this feature off on all devices.

4. Updating Antivirus and Firewall Protection

Just like your house needs regular upkeep and maintenance, your antivirus and firewall protection systems also require attention. Keeping them updated helps to keep data secure and unauthorized people from getting inside the network. While you may only be accessing trusted websites, you can never be 100% sure. An antivirus system must be thorough and regularly updated to keep your system secure from any new viruses that appear. A small investment in this account will certainly go a long way for the benefit of your business.

Keep in mind, none of the antivirus software available provides 100% protection, but it certainly definitely increases the level of safety from viruses and malware attacks. It's essential to keep this shield updated. Your managed security services provider can provide additional support with 24/7 system monitoring of unauthorized activity on the company network.

5. Using a Pop-up Blocker

Without a pop-up blocker, you run the risk of accidentally clicking on a pop-up ad that could be malware or redirect you to a malicious website. Pop-up blockers are built into web browsers, but you will need to enable it to work. There may be times when the pop-up blocker needs to be turned off, but don't leave it turned off.

6. Clearing Cache and Cookies

Websites track your browsing to learn more about you. Companies use this information to provide you with the information they think you want when you revisit the website. Do you think it's a coincidence that a product you've recently looked at on Amazon appears on a website you visit a few days later? It's no coincidence. To prevent this from happening, you will have to clear your browser cache and delete unwanted cookies. This will help limit the undesired advertisements that you see cropping everywhere. While you can do this manually, there are also options to do this automatically. To ensure that continuous log-in requirements do not hassle you, you can choose to whitelist websites that you regularly access — keeping you from having to re-login every time.

7. Using a VPN

Unlike private browsing, which prevents your browser from storing information on your computer but still allows sharing between your computer and ISP, a VPN encrypts your internet traffic and identity online. Most companies these days have a VPN, and if you don't, you should invest in one.

8. Enabling No Tracking

While on the web, it always seems like someone is keeping an eye on your movements. If you follow the tips that you read here, your web browsing experience can become as safe as it can be. Do you know that you can even send a "do not track'"request to different websites that keep bothering you with their advertisements wherever you go? However, it's sad that most of them do not usually retrace their steps and continue doing what they do. But making your choices and priorities clear at the onset is the best you can do, so do that!

9. Ensuring Compliance

While you can follow best practices, your company must have clear guidelines and policies around browsing behavior on company computers and networks. This is required to avoid any security breach and non-compliance by employees. Guidelines and policies help employees understand what they can and can't do on company devices.

In Conclusion

Once you begin following best practices for web navigation, you reduce your risk of being attacked. There are many ways to protect your browser and browsing experience online, and most of them are self-managed. Take responsibility for your company's security. Developing safe browsing habits will help you steer clear of any cyber threats today and tomorrow.

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

6050 Corporate Way
Indianapolis, IN 46278
(866) 863-2266

learnmore@visualedgeit.com
www.visualedgeit.com
@visualedgeit