CYBERSECURITY AWARENESS MONTH

bitwarden

Anatomy of Cybersecurity: How to Stay Secure at Work & at Home

Table of Contents

To share more security advice with users, and raise overall awareness of internet safety, Bitwarden joins the National Cyber Security Alliance and Cybersecurity and Infrastructure Agency (CISA) to support Cybersecurity Awareness Month 2023.

Launched in 2004, the program aims to raise awareness on cybersecurity issues and promote a safer and more secure online experience for everyone. Some key themes for this year include using strong passwords and a password manager, enabling multi-factor authentication, updating software, and recognizing and reporting phishing.

Throughout the month of October, Bitwarden and other participating organizations will provide resources across a range of topics that help businesses and individuals stay safe. Bitwarden is committed to this mission and looks forward to building more awareness around key cybersecurity topics.

Concerned About Cybersecurity? 4 Easy Steps for Staying Secure

Cybersecurity has become one of the biggest hot topics both inside and outside of technology circles over the last two years. From securing learning devices due to a rise in digital learning during the COVID-19 pandemic, to coping with the fallout of high-profile breaches of national infrastructure such as the Colonial Pipeline, there is a seemingly endless newscycle dedicated to cybersecurity mishaps and concerns.

And with this onslaught of negative news, it can be easy for everyday individuals to become overwhelmed and to feel powerless in the face of the “insurmountable” threats posed by cybersecurity. But in actuality nothing could be further from the truth, and it is possible and easy to get a handle on your own online safety.

With all of the jargon that is typically thrown around in relation to cybersecurity there is a longstanding misperception that cybersecurity is beyond everyday people and that it should be left to the professionals. Moreover, there is a prevailing sense among the public that breaches are simply a fact of life and that we should just learn to deal with them. But this just isn’t true. In fact, everyday people have a huge role to play in cybersecurity threat prevention, detection, and remediation. For example, according to IBM, 95% of breaches have human error as a main cause. Therefore, everyday day technology users are very much the first line of defense when it comes to thwarting cybercrime. Unfortunately though, many individuals are not aware of some of the best practices for boosting cybersecurity and how easy they are to use.

With that, here are a few key best practices that everyday people can implement today to enhance their own cybersecurity and create a more secure world for everyone.

Update Your Passwords and Use a Password Manager

Having unique, long and complex passwords is one of the best ways to immediately boost your cybersecurity. Yet, only 43% of the public say that they “always” or “very often” use strong passwords. Password cracking is one of the go-to tactics that cybercriminals turn to in order to access sensitive information. And if you are a “password repeater,” once a cybercriminal has hacked one of your accounts, they can easily do the same across all of your accounts.

One of the biggest reasons that individuals repeat passwords is that it can be tough to remember all of the passwords you have. Fortunately, by using a password manager, individuals can securely store all of their unique passwords in one place. Meaning, people only have to remember one password. In addition, password managers are incredibly easy to use and can automatically plug-in stored passwords when you visit a site.

Watch Out for Phishing

Phishing – when a cybercriminal poses as a legitimate party in hopes of getting individuals to engage with malicious content or links – remains one of the most popular tactics among cybercriminals today. In fact, 80% of cybersecurity incidents stem from a phishing attempt. However, while phishing has gotten more sophisticated, keeping an eye out for typos, poor graphics and other suspicious characteristics can be a tell tale sign that the content is potentially coming from a “phish.” In addition, if you think you have spotted a phishing attempt be sure to report the incident so that internal IT teams and service providers can remediate the situation and prevent others from possibly becoming victims.

Enable MFA

Enabling multi-factor authentication (MFA) – which prompts a user to input a second set of verifying information such as a secure code sent to a mobile device or to sign-in via an authenticator app – is a hugely effective measure that anyone can use to drastically reduce the chances of a cybersecurity breach. In fact, according to Microsoft, MFA is 99.9 percent effective in preventing breaches. Therefore, it is a must for any individual that is looking to secure their devices and accounts.

Activate Automatic Updates

Making sure devices are always up-to-date with the most recent versions is essential to preventing cybersecurity issues from cropping up. Cybersecurity is an ongoing effort, and updates are hugely important in helping to address vulnerabilities that have been uncovered as well as in providing ongoing maintenance. Therefore, instead of trying to remember to check for updates or closing out of update notifications, enable automatic update installations whenever possible.

The Anatomy of a Data Breach: What Are They and What Should You Do When You Spot One?

Arguably no phrase has dominated the tech world the last 24 months more than the term “data breach.” From breaches that have impacted critical infrastructure like the Colonial Pipeline to hackers compromising healthcare records at UC San Diego Health, the last two years have been saturated by headlines of cybersecurity mishaps. Yet, despite the prevalence of the breach-centric newscycle, many everyday individuals may not know what exactly a data breach is, how they typically start, and why they occur.

According to IBM, the average time it takes to identify that a breach has occurred is 287 days, with the average time to contain a breach clocking in at 80 days. And with 81% of businesses experiencing a cyberattack during COVID, it is essential that individuals are familiar with the anatomy of a data breach so that they can keep their data, as well as their colleagues and customers’ data, safe.

With that in mind, here is some helpful background on what data breaches are and why they are so problematic.

What is a data breach?

While it may seem like a complex concept, once the jargon is removed, a data breach is actually really straightforward to explain. According to Trend Micro, a data breach is “an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner.” And while data breaches can be the result of a system or human error, a vast majority of data breaches are the result of cyber attacks, where a cyber criminal gains unlawful access to sensitive system data. In fact, 92% of the data breaches in Q1 2022 were the result of cyberattacks.

What kind of data can be breached?

Unfortunately, cyber criminals look to get their hands on any information that they possibly can ranging from more obvious sensitive information such as social security numbers and credit card information to more obscure data like past purchase history.

What are some of the tactics used to execute data breaches?

Cybercrime is getting more sophisticated each day. However, cyberattack tactics do not have to be cutting-edge or advanced in order to be very effective. Here are a few examples of popular tactics used by cybercriminals:

- **Phishing**: Phishing is when a cybercriminal pretends to be a legitimate party in hopes of tricking an individual into giving them access to personal information. Phishing is one of the oldest tricks in the book for cybercriminals but it is just as effective as ever. For

example, 80% of security incidents and 90% data breaches stem from phishing attempts.

- **Malware**: Another tried-and-true method for cybercriminals is malware. Malware is malicious software that secretly installs itself on devices – often by way of a user engaging with fake links and content – and quietly gains access to the data on an individual's device or a business network.

- **Password Attack**: Through password attacks, cybercriminals look to gain access to sensitive data and networks by way of "cracking" user passwords and using these credentials to get into networks and extract data from a given network.

How to spot a possible breach?

The best way to stop a data breach is to stop it before it even starts. This includes taking steps from making sure passwords are long and complex to reporting suspicious emails. If you do suspect that you have been the victim of a breach immediately contact your IT department or device provider to notify them and follow subsequent protocols to help them scan, detect, and remediate any issues that exist.

Cybersecurity in the Workplace: 4 Tips to Keep Your Business Safe and Secure

Keeping information safe and secure is challenging developments for businesses of all sizes over the last few years. Expeditious shifts from in-person to online to hybrid workplaces forced companies to change, or at least reexamine, their cybersecurity practices and protocols, and far too often they weren't prepared. In fact, according to CyberEdge's Cyberthreat Defense Report, 85% of organizations suffered from a successful cyberattack in 2021.

Now, businesses who have suffered cyberattacks along with companies who've been fortunate enough to avoid being a victim of breaches and hack are looking at ways they can bolster their defenses and safeguard their data. But which plans, practices, and services should these organizations invest in?

Below are 4 steps businesses of all shapes and sizes can take to better protect themselves against cyber attacks:

Identify “Crown Jewels” of Your Business

Understanding what information cybercriminals are after most is essential to combating cyber attacks. Therefore, creating an inventory list of the valuable data and assets within your organization, including manufacturer, model, hardware and software information, is of the utmost importance. In addition, take note of who has access to important data and information while also accounting for all storage locations. This practice will ensure that business leaders have a track record of accessibility so that they know where to look in case of a vulnerability or breach.

Protect Assets by Updating and Authenticating

At the end of the day, protecting your data and devices from malicious actors is what cybersecurity is all about. In order to accomplish this, make sure your security software is current. Investing in the most up to date softwares, web browsers, and operating systems is one of the best defenses against a host of viruses, malware, and other online threats. Furthermore, make sure these devices have automatic updates turned on so employees aren’t tasked with manually updating devices. Additionally, make sure all data is being backed up either in the cloud or via separate hard drive storage.

Another important way to keep your assets safe is by ensuring staff are using strong authentication to protect access to accounts and ensure only those with permission can access them. This includes strong, secure and differentiated passwords. According to a 2021 PC Mag study, 70% of people admit they use the same password for more than one account. Using weak and similar passwords makes a hacker's life a lot easier and can give them access to more materials than they could dream of. Finally, make sure employees are using multi-factor authentication. While this may result in a few extra sign-ins, MFA is essential to safeguarding data and can be the difference between a successful and unsuccessful breach.

Monitor and Detect Suspicious Activity

Companies must always be on the lookout for possible breaches, vulnerabilities and attacks, especially in a world where many often go undetected. This can be done by investing in cybersecurity products or services that help monitor your networks such as antivirus and antimalware software. Moreover, make sure your employees and personnel are following all established cybersecurity protocols before, during, and after a breach. Individuals who ignore or disregard important cybersecurity practices can compromise not only themselves, but the entire organization. Paying close attention to whether your company is fully embracing all of your cybersecurity procedures and technology is incumbent upon business leaders.

Have a Response Plan Ready

No matter how many safeguards you have in place, the unfortunate reality is that cyber incidents still occur. However, responding in a comprehensive manner will reduce risks to your business and send a positive signal to your customers and employees. Therefore, businesses should have a cyber incident response plan ready to go prior to a breach. In it, companies

should embrace savvy practices such as disconnecting any affected computers from the network, notifying your IT staff or the proper third-party vendors, and utilizing any spares and backup devices while continuing to capture operational data.

Cybersecurity In The Home: 3 Steps Households Can Take

The COVID-19 pandemic forced millions of Americans to embrace working from their own home; a concept they had limited or no experience with at the time. And while many employees have returned to the office, a recent University of Chicago study found that 72% of those workers surveyed would like to continue working from home for at least 2 days a week, and 32% said they would like to work from home permanently. In this new reality, having your household safe and secure from cyber threats needs to be a top priority.

In this increasingly wireless world, the steps households should take in terms of cybersecurity have changed. Most homes now run networks of devices linked to the internet, including computers, gaming systems, TVs, tablets, and smartphones that access wireless networks. Thus, having the right tools in place will instill confidence that your family members can use the internet safely and securely for personal and work related endeavors.

Below are 3 steps households can take to better protect themselves against cyber attacks:

Secure Your Wireless Router

Using a wireless router is an increasingly convenient way to allow multiple devices to connect to the internet from different areas of your home. However, unless your router is secure, you risk the possibility of individuals accessing information on your computer, and worse, using your network to commit cybercrimes. Needless to say all wireless devices using this router are vulnerable if your router is not protected.

Some simple ways to secure this piece of hardware include changing the name of your router. The default ID is typically assigned by the manufacturer, so changing your router to a unique name that won't be easily guessed by others is a simple way to keep your router protected. Another important step is changing the preset passphrase on your router. Leaving the default password in place makes it significantly easier for hackers to access your network. In fact, according to NCA's 2021 Oh Behave! Report, only 43% of participants reported creating long and unique passwords for their online accounts "very often" or "always". Additionally, almost a third (28%) stated that they didn't do this at all. Embracing unique and strong passwords is a huge and simple step to securing your home from all types of cyber threats.

Install Firewalls and Security Softwares On All Devices

Firewalls are essential because they help keep hackers from using your device which otherwise could result in your personal information being sent out without your permission. They guard and watch for attempts to access your system while blocking communications with sources you don't permit. Installing a firewall on wireless routers is a necessity. Furthermore, make sure all devices that are connected to the wireless network have security software systems installed and updated. Many of these gadgets have automatic update features, so households should make sure they are on for all available technology. The most up to date security softwares, web browsers, and operating systems are the best defense against online threats such as viruses and malware.

Back Up All Household Data

While steps can be taken to avoid your network, devices and accounts being hacked or compromised, they can never be 100% effective. With that being said, households need to embrace backing up data, especially as it relates to important information. Users can protect their valuable work, photos and other digital information by making electronic copies of important files and storing them safely. This can be done using cloud software in addition to manual storing devices like USBs. Regardless, storing data in an alternative location that is safe and secure provides another layer of protection.

Taking simple, proactive steps to keep family, friends and yourself safe from cyber criminals inside your household should no longer be viewed as optional but rather a necessity. Between technological devices being introduced and updated at a rapid pace and employees continuing to embrace working from home in some capacity, everyone has an ethical responsibility to actively minimize the risks of breaches and attacks inside their home.

Take the first step to better protect your sensitive data from potential data breaches and try the Bitwarden password manager for free today! For advanced enterprise features, sign up for a free 7-day enterprise trial