6 Cybersecurity Myths Debunked

There are a lot of myths flying around about cybersecurity. We'll go over the most common cybersecurity myths and debunk them so we can stay safer online.

While more and more people are making better choices when it comes to protecting their data, there appear to be many cybersecurity myths that hold some people back.

Let's examine the most common security myths one by one and debunk them so we can be safer online. Feel free to share this article with friends and family!

Myth 1: Cybersecurity is too hard, so why bother?

An unfortunately common belief we hear from people is that cybersecurity is so complicated that it isn't even worth trying. According to the Oh Behave! survey, only 60% said they believed online safety is worth the effort. However, there are many simple ways to improve your protection, and you don't need to be a tech expert.

You can also start small by avoiding reusing passwords and learning to recognize scam messages. You are probably already using some tools, such as multifactor authentication. While it requires a little effort, we think you'll be surprised at how easy it is to use tools like password managers. Use our free resources to learn more.

Although there is no way to be completely "cyberproof," a few behavioral changes can significantly improve your online safety.

Myth 2: It doesn't matter if my device or account gets hacked.

Along with the myth that cybersecurity isn't worth the effort, people think they have nothing worth protecting and that some people believe that it doesn't really matter if their accounts are breached because the data isn't critical. Here's the thing – data collection is a multibillion-dollar industry. Even if you don't think your data is valuable, it is.

You might think an account isn't important, say, on social media. However, if a hacker gains access to your social media, they may impersonate you and attempt to scam your friends.

Because of this, you should follow great security practices for every account, even silly or fun ones. Make security a habit and enjoy peace of mind.

Myth 3: Password managers aren't safe because what if the password manager gets hacked?

Password managers are great, but sometimes people express concerns about storing all their passwords in one place. However, high-quality password managers are the safest way to store your passwords. These programs also ensure that

you're using strong, unique passwords for each of your accounts. Password managers are not like putting all your eggs in one basket because baskets don't have MFA or zero-knowledge architecture!

Because of the technology password managers use, the password manager company doesn't even know your master password. This is why you want your master password to be long and unique! When you enable MFA on your password manager, it becomes even more secure.

There have been incidents when password manager companies get hacked. However, when you use a strong master password and MFA, you can maintain your security even in these situations. This is why password managers are safer than notebooks, sticky notes, or documents saved on your computer.

Myth 4: I have a strong password, so I don't need to worry about anything else.

It's great if you have a strong password that is at least 16 characters long and a blend of letters, numbers, and special characters. However, this is just one part of being a cybersecurity superstar.

For one, every account and device needs its own password; that is, don't reuse your password, regardless of how strong it is. If you reuse passwords, it means that if one of your accounts is hacked, all your other accounts are at risk. To store all your unique passwords, we recommend a password manager!

Next, it is recommended that you enable MFA for every account. This doubles up your protection beyond your password. The few seconds required to enter a code sent to your phone or scan your face is well worth the extra protection.

TL;DR: You need a unique, strong password for every account, and turn on MFA to maintain maximum security for your online life.

Myth 5: Phishing emails are easy to spot due to poor grammar and misspellings.

Oftentimes, you can spot phishing and other scam messages because of generic greetings, misspellings, and bad grammar.

Since the widespread use of artificial intelligence and large language models (LLMs), though, scammers have become much more sophisticated and more challenging to identify. The grammar and spelling of phishing emails have improved significantly in just a few years.

Some scam messages can appear almost identical to messages from trusted sources, such as Amazon or Facebook. If a message is trying to get you to click on a link or download an attachment, take a moment. If the message was sent to your work email, report it to the Metro ITS Help Desk or use the “Report Phishing” button. If the suspicious message was sent to your personal email, check to see if the sender has a strange email address. Many email services today let you report phishing attempts if something doesn't feel right.

Beyond misspellings and poor grammar, the primary indicator of a scam message is a sense of urgency. Is the message unexpected? Is it trying to get you to act quickly without thinking? Even if your high school English teacher would give the message an A, you should be suspicious of these urgent messages.

Myth 6: A VPN is all you need.

A virtual private network (VPN) is a great tool for staying safe, especially when using public wi-fi. However, VPNs aren’t security magic – you still need to use strong, unique passwords and avoid clicking on scam links to maintain your protection.

A VPN encrypts your web surfing and helps protect your data. However, this is only one part of security and it is just one tool in your cybersecurity toolbox.

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.