|  |
| --- |
| https://sagoknowbe4assets.z21.web.core.windows.net/tamus-oit-banner-sm.jpg |
| |  |  | | --- | --- | |  | **Security Tips - Cybersecurity Myths, Busted!**  It’s time for a pop quiz: Which of the following is a myth?   1. Only people in high-power positions are targets of cybersecurity attacks. 2. High-tech hackers pose the highest threat to your organization. 3. Cybersecurity is a highly technical process that only your IT department can handle. 4. Security awareness only really matters when you’re at work. 5. Smart devices are rarely targeted by cybercriminals.   Did you find the myth? Hopefully you did, because this was a trick question! Each of these is a common cybersecurity myth. Read on to learn the truth behind these misconceptions:  **Myth #1: Only people in high-power positions are targets of cybersecurity attacks.** Executives and administrators are prime targets for cybercriminals, but that doesn’t mean they’re the only targets. Scammers attack every level of an organization, looking for gaps in security. After all, it only takes one hacked machine to access your entire network.   **Myth #2: High-tech hackers pose the highest threat to your organization.** You may imagine a cyberattack as the use of highly sophisticated technology to break down firewalls and decode user passwords. But in truth, it is much more likely that Dave wrote his password on a sticky note and it fell into the wrong hands. Human error is an easy target for cybercriminals, so stay alert!   **Myth #3: Cybersecurity is a highly technical process that only your IT department can handle.** The security tools that your IT department manages are important, but technology can only do so much. These security measures can’t stop an employee from sending sensitive information within an email. Creating a human firewall, made up of each and every employee, is essential to the security of your organization. Security is everyone’s responsibility.   **Myth #4: Security awareness only really matters when you’re at work.** Your organization’s at-work policies and compliance regulations may not be necessary in your home life, but security awareness still matters. Scammers could phish your personal email for bank accounts, login credentials, or even personally identifiable information, which can be used to perform identity theft.   **Myth #5: Smart devices are rarely targeted by cybercriminals.** Nearly everyone has a smartphone and many people use smart devices throughout their homes. From smart speakers to security cameras to lightbulbs, all of these gadgets connect to the internet. As these devices become the norm, cybercriminals happily accommodate. Treat smart devices the same way you would treat any other computer. Always use strong passwords, install antivirus and anti-malware software and keep these devices up-to-date with the latest security patches.   Believe it or not, you are the key to keeping your organization secure!  **Stop Look Think** - Don't be fooled | |