# CYBERSECURITY

Data privacy is an ever-changing field, and governments across the United States are enacting new laws and regulations to help safeguard American personal information in an increasingly digital society.

Indiana has not been immune to the emerging cybersecurity threats. According to the Federal Bureau of Investigation (FBI), more than 11,000 Hoosiers became victims of an online cyberattack during 2022 alone, amounting to more than $73 million in losses. Cyberattacks are also a major threat for Indiana governments, schools, businesses and other organizations. An Indiana cybersecurity incident reporting law went into effect in 2021, requiring all political subdivisions to report cybersecurity incidents to the Indiana Office of Technology.

As attacks continue to become more commonplace and sophisticated, it is important that all Indiana families and businesses know how to identify and avoid online threats. Hoosiers can learn more about cybersecurity and how to better protect their data privacy by reviewing the tips below and by visiting the Indiana Cybersecurity Hub.

## QUICK TIPS

- Create strong passwords of at least eight characters long, and use combinations of uppercase and lowercase letters, numbers and punctuation.
- Use different usernames and passwords for your accounts, and be sure to implement multi-factor authentication.
- Do not open or download files, answer questions or follow tasks in emails sent from unknown or unsolicited senders. Never send personal or financial information to them.
- Keep antivirus programs updated on all devices.
- Back up important files to an external hard drive, flash drive or online cloud storage account.

---

# CYBERSECURITY TIPS

## PASSWORDS

Passwords are keys to personal information and data. Having a strong password will help keep intruders out.

- Passwords should be at least eight characters long and use combinations of uppercase and lowercase letters, numbers and punctuation.
- Never use the same username and password on multiple websites.
- Never use personal information such as names, ages, birthdays or a pet's name.
- Avoid entering personal passwords on shared devices.
- Implement multi-factor authentication on your accounts, including email, social media, online shopping, financial services, gaming and entertainment.

## SHOPPING

Online shopping sales have steadily increased over the past decade and now make up more than 10 percent of total U.S. retail trade revenue, which means sensitive financial information is being transmitted and stored online more and more. Protect this information by following these tips.

- Before purchasing an item, check the website for security and authentication notices.
- Be aware of severely undervalued prices.
- On auction sites, check the seller's reputation, read reviews about the seller and thoroughly read the item's description.
- At checkout, use a secure payment method such as a debit or credit card.
- Avoid shopping on a public computer or public Wi-Fi network.

## COMMUNICATION

Today, a lot of information is shared through forms of online communication. Practicing discretion will help keep this information in the right hands.

- Never open, answer or follow tasks in emails sent from an unknown or unsolicited sender.
- Never send personal or financial information to an unknown or unsolicited individual.
- Do not download files or programs from an unknown company or source.
- Change social media privacy settings so only trusted individuals can see posted information.
- Limit the amount of personal information shared on social media.
- Never share financial information, account information or passwords on social media.

## DEVICES

According to the Pew Research Center, 97 percent of Americans own a cell phone, half own a tablet computer and about 75 percent own a desktop or laptop computer. These devices hold personal information, so protecting them from cybercriminals is important.

- During travel, always keep laptops and mobile devices nearby or locked with a strong password, especially if they are not within reach.
- Never answer calls or messages from unknown contacts.
- Protect devices with strong passwords.
- Encrypt all confidential or personal information.

## SOFTWARE

In addition to caution and strong passwords, software programs can also provide a layer of protection for devices. Research the programs and decide which one is the best fit for the household or business.

- Back up important files to an external hard drive, flash drive or online cloud storage account.
- Install antivirus software that detects and removes viruses from electronic devices.
- Keep device operating systems, applications and security software updated. Turn on automatic updates.
- Install a firewall to block harmful material.

## WORKPLACE DO'S AND DON'TS

### *Workplace Do's*

Remembering to practice digital safety tips at work could prevent a company from having to spend millions of dollars to deal with the consequences of a cyberattack.

- Understand common terminology about cybersecurity. A great way to prevent cyberattacks is understanding what they are and how they work.
- Use passwords that are at least eight characters long and use combinations of uppercase and lowercase letters, numbers and punctuation. A strong password reduces the possibility of cybercriminals finding personal information.
- Keep antivirus programs updated on all electronic devices. These programs can detect and remove possible cyberattacks.
- Change social media privacy settings so only trusted individuals can view posts.
- Regularly change passwords for every account.
- Lock computers when leaving the desk or workstation. Leaving computers unlocked allows unauthorized individuals to access sensitive work-related information.
- Verify the email sender before opening a message. The message may seem legitimate, but it could hold a virus.
- Ask employers about available cybersecurity training courses.
- During travel, always keep laptops and electronic devices nearby or locked with a strong password, especially if they are not within reach.

### *Workplace Don'ts*

Avoiding a few common mistakes can make the workplace more secure and decrease the likelihood of a cyberattack.

- Never use the same username and password on multiple websites. Using the same password can increase the chance of cybercriminals stealing information from multiple accounts.
- Never use personal information like names, pet names or birthdates in passwords.
- Never share passwords with others.
- Never click on links or follow tasks in emails from unknown or unsolicited sources.
- Never download images, documents or software from unknown or unsolicited sources.
- Never share sensitive work-related information with unauthorized individuals.
- Never keep computers on all the time.