Girl Scout Cyber Awareness Challenge

In collaboration with the U.S. Department of Homeland Security

Want to explore cybersecurity and protect yourself and others online?

Join Girl Scouts of the USA, the U.S. Department of Homeland Security (DHS), DHS's Cybersecurity and Infrastructure Security Agency (CISA), and CYBER.ORG this summer for the Cyber Awareness Challenge!

Now through October 24, 2021, complete the activities and submit a description of your work to receive a certificate of recognition from DHS.

Check out www.cyber.org/girlscoutcybersummer and www.girlscouts.org/cyberawareness for resources to help with the activities!

The threat of ransomware is real.

Ransomware is a type of malware that denies the victim (the people or organizations being attacked) access to their data until they pay a ransom. It's often the malware (short for malicious software) of choice for cybercriminals. Ransomware attacks can shut down entire computer networks and slow, or even stop, the victim's daily operations.

In 2020, victims paid ransomware attackers $350 million. The number of these attacks on cities and organizations, such as hospitals, schools, small businesses, and utilities, has been increasing in recent years. When an organization or government is attacked by ransomware, it prioritizes getting its data back as quickly as possible. In some cases, paying the ransom appears to be the quickest and cheapest way to restore data; however, cybersecurity experts discourage paying a ransom after an attack for three main reasons:

1. Despite what the ransomware promises, paying the ransom does not guarantee that the data will be restored.
2. Paying the ransom incentivizes cybercriminals to continue using ransomware, because it "works."
3. Paying the ransom might mean that you're funding other illegal operations.

Although governments, businesses, and organizations are often the targets of ransomware attacks, individuals are also at risk. Cybercriminals can target anyone with an internet-connected device or with important data stored on their network. In some cases, personal attacks can be even more harmful to individuals, because many users don't have a cybersecurity plan in place. If you ever become a victim of ransomware attack, report it to the Cybersecurity and Infrastructure Security Agency at https://us-cert.cisa.gov/report.

Complete these ten actions to protect yourself and others online.

Check out www.cyber.org/girlscoutcybersummer and www.girlscouts.org/cyberawareness for resources to help with the activities.

1. **Explore cybersecurity with Girl Scouts.** Have you earned a Cybersecurity badge or participated in a Cyber Challenge? If so, awesome! You're on your way to being a cybersecurity expert. If not, get started with an activity on Girl Scouts at Home for your grade level. Then, if you want, head over to the Girl Scout shop for more information to complete the Cybersecurity badge series.

    - Grades 6–8: Cadette—inventory your digital presence
    - Grades 9 and 10: Senior—identify functions and privileges
    - Grades 11 and 12: Ambassador—guard your movements

2. **Identify risks in your personal data.** Everything you do online leaves a trail of digital footprints. Just like a detective, a hacker can piece them together to learn about you. Your personal data may be vulnerable to cyberattack if you aren't very careful about how you use digital devices, like phones, tablets, and computers. Make a list to examine what you do online every day; how might your personal information be vulnerable to a cyberattack? Consider how what you do offline makes your

personal information vulnerable, too, like sharing your password or losing your school ID. Remember that you have control over your digital footprint—you can be savvy when you're browsing the internet and think before you post.

3. **Update your passwords.** Hackers have programs that run through dictionaries to identify and try millions of passwords to hack into people's accounts in just minutes. The programs also search books, movie scripts, and song lyrics or scan social media sites for clues, like birthdays and pets' names. Because hackers expect people to follow grammar rules for capitalizing letters, the strongest passwords have numbers, special characters, and capital letters in unusual places. It also takes a hacker's program longer to guess a long password than a short one. Some experts even suggest choosing four random, unusual words that make no sense together to create a passphrase, like tunaFlipflopsnoreSHINY.

4. **Add multifactor authentication to make your accounts even more secure.** Because passwords can be easy to hack, cybersecurity specialists have added more layers to get into an account beyond your username and password. This is called multifactor authentication (MFA). Some send a randomly generated code to your cell phone, some ask for a fingerprint or scan your eye, and some have an actual physical "key" that looks like a USB stick or flash drive. Review your account and system settings to see if MFA is an option. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone or an authenticator app.

5. **Review your privacy settings.** Social media, as well as other apps and platforms, often have privacy settings that allow you to control who can see what you share. You can decide to make your accounts private, only sharing information with people you're connected with. You can often control the settings on individual posts, choosing to share with just one person, a group, or the public. When you know what information you're sharing (and with whom), you can make sure to only share public information with people you know and trust. This decreases the chances of someone using your personal data against you in the future.

6. **Keep your devices up-to-date.** More and more devices—from coffee makers and washing machines to lightbulbs and headphones—can be connected to the internet. This network of connected devices is called the Internet of Things (IoT). The IoT network allows objects to be controlled remotely, and it's getting bigger every day. Billions of connected devices can make life easier for people but can also make those devices less secure. That's why cybersecurity experts are working to make the IoT as safe as possible. Do a bit of digital summer cleaning and check all of your devices and smart appliances. Update them to the latest software, and delete any accounts or apps that you no longer need. You can also put anti-virus software on your computer that looks for viruses and gets rid of them before they can cause harm.

7. **Back up your data.** Backing up your data on a regular basis ensures that you don't lose important information if your device breaks or you're hacked. You can store important documents, photos, and other files on a secure cloud system that's made for backing up. Local backups, like a hard drive or even a USB, can also hold your

data offline. Backing up your data regularly reduces your risk and keeps your data safe in case anything happens. You can also back up your files manually or find a way to automate your backup system.

8. **Clean up your inbox.** Hackers try to trick people by sending emails with bad links, harmful attachments, or requests for money and private information. This kind of email is called phishing. If you click the link or download the attachment, a computer virus can sneak into your computer, spreading bad code and destroying information. Then your computer can spread the virus to other computers that you're linked to. Look through your email accounts—do all the emails in your inbox seem legitimate? Can you find any that are suspicious, like phishing, spam, or clickbait? Delete any spam and make sure not to click on any links or attachments.

Here are some questions to consider if an email is legitimate:

- **Does it ask you to confirm personal information?** A real website or business wouldn't ask you to confirm personal information, like your login and password. Hackers may send emails that seem like they're from a website you use and trust.
- **Is the email or website one that you know and trust? Take** a look at the sender's email address and any links—they may be just a little bit different from the company's official email address and website. For example, a hacker might change girlscouts.org to girlsscouts.com or girlscout.org. If you're suspicious of a link, hover your cursor over it, but don't click, to see the address where you'd go if you clicked.
- **Does it use poor spelling and grammar?** A real email from a website you use wouldn't have lots of spelling or grammar mistakes. It's also likely that they wouldn't say "Dear customer."
- **Does it seem urgent?** Emails may be written to make you think there's an emergency or that you can get free money.

9. **Plan your digital future**. Five or ten years from now, what do you imagine you'll be doing? Working? Going to college or graduate school? Starting your own company? It's exciting to think about your future and important to consider how what you do online today can affect your future opportunities. It's not just hackers who look at digital footprints. Colleges, graduate schools, and employers will often do an internet search before offering a place at their school or a job. Even new friends may do a search. What do you plan to do in your future? Have you considered cybersecurity as a career? No matter what you do, how could what you do online now affect how people perceive you in the future? Reflect on what you've learned, and find out about different jobs related to cybersecurity. Then create a list of next steps and cyber habits to lead you to your desired future digital profile.

10. **Create a ransomware awareness campaign to share with your community.** Raising awareness about safeguarding personal information benefits society by making it harder for hackers to steal information. What creative ways can you teach others about ransomware and motivate them to embrace cyber habits, like updating their passwords, turning off their webcams, and using social media wisely? Develop an awareness campaign about the importance of ransomware and cybersecurity to share with a community that you're a part of, like your school, town, or community center. Create materials to share your message in any format that will reach your audience, such as a poster, flyer, digital presentation, comic strip, article, or short video. Then share your campaign with your community to engage people in a conversation about ransomware and cybersecurity. Finally, find ways you can work together to create a safer digital world for all.

    Check out page 6 for more information and ideas to plan your campaign.

Finally, complete the challenge and submit a description of your campaign!

How to Create Your Ransomware Awareness Campaign

1. Choose an audience. All of us are part of different communities, from our family and friends to our school, town, and even the world!

Choose an audience to reach with your campaign, like members of your local government, community center, or school. Decide who you want to spread awareness to, such as other youth, adults, teachers, or community leaders.

Once you've chosen an audience, consider what some of their barriers may be to being cyber secure. Why might your audience be vulnerable to cyberattacks like ransomware? How can you help them become more aware in the digital world?

2. Decide which message to share. Reflect on what you've done and learned throughout the challenge. What's most important to tell your audience about cybersecurity? What do those people need to know about ransomware?

Choose one or more cyber habits that you'd like your audience to adopt and to develop your message. Make sure to answer these questions about ransomware:

- What is ransomware?
- Why is ransomware a problem?
- What effect does ransomware have on individuals?

How can we protect ourselves and our community from ransomware attacks?

3. Create materials. How can you reach your target audience? What can you make or do? Choose a way to share your message in person, virtually, or a combination of the two.

Then create materials for your campaign. The format is up to you, but make sure it's both accessible and engaging for your audience!

You might:

- Film or animate a video
- Design infographics or posters
- Develop a guide or toolkit
- Draw a comic
- Make an event or workshop materials
- Write an article
- Build a website

4. Share your ideas with your community. Once you've created your campaign, it's time to share it with your community!

Use the materials you created to start a conversation about cybersecurity and ransomware. Share your new knowledge and habits that others can adopt to protect themselves, their data, and devices.

You might:

- Present your campaign to your local government
- Hold a community conversation or panel discussion
- Host a community event
- Hold a community workshop
- Publish your ideas in a local newspaper, in a newsletter, or online

Bonus: Create a cyber action plan with your community.

What next steps can you take together as a community? To expand your campaign, brainstorm and put together a plan for everyone in your community to have a role in making a difference for themselves and others online.

Need more information on cybersecurity and ransomware?

Check out these resources from the Cybersecurity and Infrastructure Security Agency and Cyber.org!

- Cyber Awareness Challenge resources, including cyber career profiles and tips for online privacy.
- Cyber Safety video series, with information about potential threats that you may encounter online and what you can do to stay safe.
- Guides and services, including tips and best practices for individuals, organizations, and technical staff to guard against ransomware.
- Fact sheets and infographics, featuring easy-to-use, straightforward information to help organizations and individuals better understand the threats and consequences of a ransomware attack.
- Trainings and webinars with information on ransomware for technical and non-technical audiences, including managers, business leaders, and tech specialists.
- *Ransomware Guide—Prevention Best Practices and Response Checklist* for best practices and ways to prevent, protect, and respond to a ransomware attack.
- CISA INSIGHTS—Ransomware Outbreak with background information on specific cyber threats, the vulnerabilities they exploit, and mitigation activities.
- Ransomware Reference Materials for K–12 with information about increased cyberattacks on K–12 schools and remote learning, as well as best practices to avoid becoming a victim of ransomware.

Be a savvy traveler this summer

Remember these tips when you head out for your next adventure:

- **Lock your devices.** Use your passcode or fingerprint to protect information on your smartphone or tablet.
- **Limit your location sharing.** Turn off location authorization on apps. Don't share photos or your location on social media while you're traveling.
- **Turn off your Bluetooth.** If you use Bluetooth to connect to a speaker at home, be sure it's turned off on your phone when you're traveling. Hackers can locate your phone through Bluetooth.
- **Turn off Wi-Fi auto connect.** If you've set your device to automatically connect to open Wi-Fi networks, turn that off. Make sure every Wi-Fi connection you use is secure.
- **Change your passwords.** Just in case someone figures out your password while you're traveling, it's a good idea to use a different one than you usually use at home. You can change it back when you get home.
- **Don't leave your digital devices unattended.** If your hotel room has a safe, put your devices in it when you aren't using them. If you must leave your devices in the car, lock them in the trunk.