women in CYBERSECURITY

WiCyS

CYBERSECURITY AWARENESS MONTH

– TOOLKIT –

Brought to you by WiCyS Tier 1 Strategic Partners:

Akamai

amazon

Bloomberg

Carnegie Mellon University
Software Engineering Institute

cisco

Ford

Google

LOCKHEED MARTIN

Microsoft

Optum

Sandia National Laboratories

SentinelOne

WiCyS Cybersecurity Awareness Month Toolkit

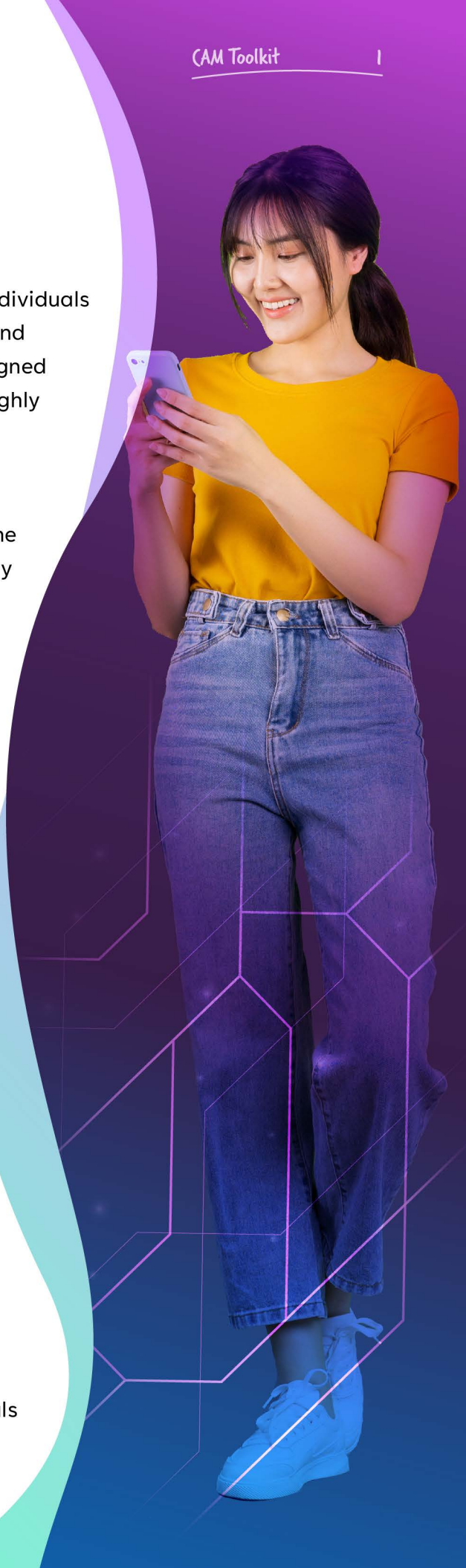
The **WiCyS Cybersecurity Toolkit** is an invaluable resource for individuals who are passionate about enhancing cybersecurity awareness and reducing cyber risk within their communities. This toolkit is designed to empower individuals with a comprehensive set of free and highly effective tools that can be easily accessed and utilized.

At the heart of the toolkit is a carefully curated collection of resources selected by our strategic partner experts that are in the field of cybersecurity. These tools are organized in a user-friendly manner, making it easy for individuals to search, find and implement basic cybersecurity measures. Whether you are a seasoned cybersecurity professional or an individual with limited technical knowledge, the WiCyS Cybersecurity Toolkit provides resources tailored to your needs.

One of the key features of the toolkit is its focus on community mobilization. It recognizes that effective cybersecurity requires a collective effort, and it provides tools that can be used to engage and educate others about the importance of cybersecurity. These tools include resources for creating awareness campaigns, organizing workshops and seminars, and developing educational materials.

The WiCyS Cybersecurity Toolkit also includes a wealth of information on best practices for protecting personal and sensitive data. It covers topics such as password management, email security, social media privacy and online banking security. By leveraging these resources, individuals can significantly reduce their risk of falling victim to cyberattacks.

The tools provided in the toolkit are constantly updated to reflect the evolving cyber landscape. This ensures that individuals have access to the latest and most effective cybersecurity measures.



Cybersecurity Awareness Month

Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month. The goal of this month is to help individuals protect themselves online as threats to technology and confidential data become more commonplace. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally.

What is Cybersecurity?

Cisco, a WiCyS Tier One Strategic Partner and industry leader, defines cybersecurity as the practice of protecting systems, networks and programs from digital attacks. These **cyberattacks** are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via **ransomware**; or interrupting normal business processes.

Implementing effective cybersecurity measures may seem particularly challenging today because there are more devices than people, and attackers are becoming more innovative; however there are simple and effective ways to defend your systems!

Cybersecurity 101

What is cybersecurity? Learn about cybersecurity and how to defend your data and applications against today's growing cybersecurity threats.

Microsoft Learn Cybersecurity is for Everyone: These beginner-level modules help learners understand concepts such as cybersecurity, Zero Trust and ransomware.

Social Engineering

No matter how sophisticated our digital controls may be, the most significant and persistent vulnerability remains human behavior. **"Social engineering"** refers to the manipulation of individuals into revealing information or taking actions that violate standard security procedures and best practices, thereby allowing unauthorized access to a system.

"Phishing" refers to the attempt to acquire personal information, such as passwords, or to trick individuals into opening a malicious attachment or clicking on a harmful link to gain access to a system. While this type of attack has traditionally been delivered via email, there has been a recent increase in the use of "vishing," which utilizes phone calls and voicemails, and "SMShing," which involves text messaging.

According to **Sentinel One**, here are some ways to reduce the risk of falling for a phishing scam:

- **Turn on anti-phishing preferences:**
  - “Safe browsing” on Chrome
  - “Block dangerous and deceptive content” on Firefox
  - “Warn when visiting a fraudulent website” on Safari

- **Look for indicators:**
  - Poor spelling and grammar errors
  - Being sent from the wrong email address
  - Sense of urgency, i.e “Your immediate attention is required”

In general, you should never disclose sensitive information such as personally identifiable information or credit card information. Avoid clicking on a link from an email or downloading an attachment; instead, go to a page from a bookmark in your browser or lookup the link in an internet search engine.

The **Take 9** campaign provides a great rule of thumb in general. If something seems out of place or too good to be true, pause for 9 seconds. This 9 second pause can keep you and your community safer! “Because we are all connected, protecting yourself online can make our country safer, too.”

Privacy

Your personal information is valuable, and protecting it is essential for ensuring your safety online. In today's digital landscape, personal data—such as your name, address, phone number and even the websites you visit—can be collected and used in ways that may expose you to risks, including identity theft and targeted scams. This is why privacy is so important. It gives you control over your own information and helps protect your identity. When we don't take steps to protect our privacy, it becomes easier for others to misuse our data or invade our personal lives.

Before you agree to anything online, like allowing cookies or signing up for a service, it's important to read the terms and conditions. These are the rules about how your data might be used. While it may seem long or boring, understanding what you're agreeing to can help protect your personal information from being misused.

Avoid sharing too much personal information online, use strong privacy settings on social media, and be cautious when clicking links or downloading attachments. By taking control of your online privacy, you can enjoy the internet safely and confidently.

- Protect your Privacy Online
- Guide to Protecting Personal Information Online
- Data Privacy

Updating Software

It is essential to keep your software up to date because updates enhance existing features, patch security flaws, add new security features, fix bug issues and improve performance for devices. It is best to install device updates as soon as they are available as this will ensure your device is protected from the latest vulnerabilities. This practice should be done for all devices, laptops, mobile devices, smart watches, earbuds, home security systems and others.

Understanding Patches and Software Updates

Password Manager

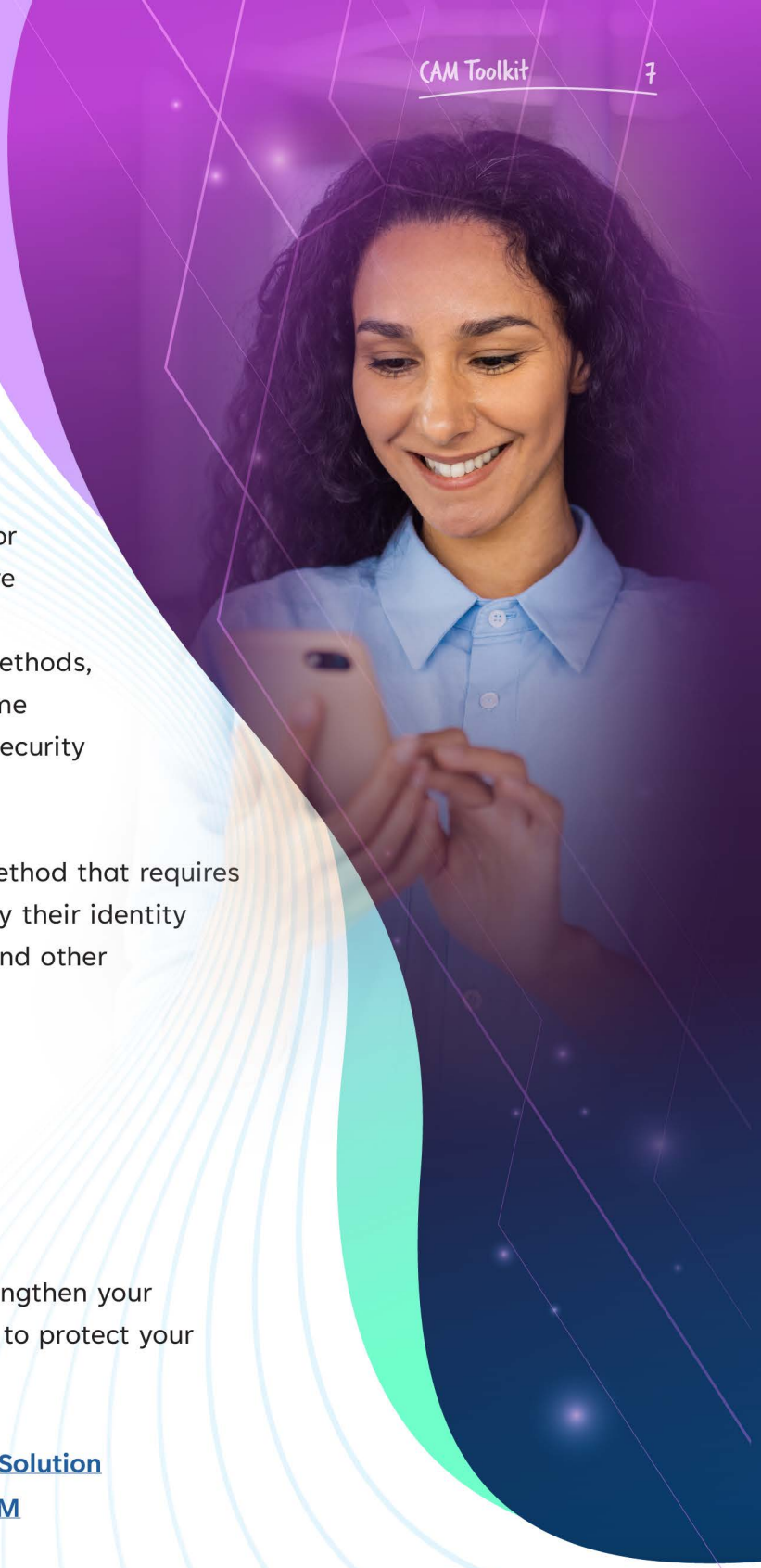
When opening a new online account, we often come across password prompts that tell us to use strong passwords or avoid repetitive passwords to stay protected from cyber threats, so we try to create unique passwords for each online account. However, when we have multiple online accounts with varying passwords, remembering them all can become daunting which is where tools such as password managers become useful.

A password manager is a software application designed to store and manage online credentials conveniently so you don't have to remember them. It can be stored on your phone, tablet, or computer and helps you create stronger passwords, which makes your online existence less vulnerable to password based attacks. It will create and store your passwords and can automatically insert them into websites and apps, saving you the need to input them manually each time you log in. Usually, these passwords are stored in an encrypted database and locked behind a master password to ensure it is securely protected. This master password provides access to your password manager account, so you'd need to keep it very safe as you can't store it in your password manager account.

Try these recommended password managers to manage your passwords and keep them secure.

- 1Password
- Dashlane
- Keeper
- RoboForm
- StickyPassword
- NordPass
- Norton

Authentication



Authentication provides an extra layer of protection to an organization by ensuring that the users accessing networks are approved to do so. In the past, usernames and passwords were sufficient to access applications or accounts. However, these two credentials alone are now too vulnerable to theft and exposure by third parties. Authentication uses various verification methods, or factors, to confirm your identity such as one-time passwords (OTPs), facial recognition, location or security questions.

Multi-factor Authentication (MFA) is a security method that requires users to provide two pieces of information to verify their identity before accessing websites, networks, databases and other network-based applications.

Use these tools from WiCyS Tier 1 partners to strengthen your passwords and set up multi-factor authentication to protect your devices and accounts.

- Akamai MFA-Multi- Factor Authentication Solution
- Amazon Multi-Factor Authentication for IAM
- Cisco Secure Access by Duo
- Google Authenticator
- Microsoft Authenticator

Use this guide to find out which websites have multi-factor authentication available: https://2fa.directory/us/

Artificial intelligence (AI)

AI technology refers to computers or machines programmed to perform tasks by simulating human thought or behaviors. It is a part of your daily life and offers many exciting opportunities, including acquiring new skills, increased knowledge and even recommendations on who to follow on social media. However, it can create problems if not used responsibly. As AI continues to evolve and play a larger role in the digital world, it is important to learn how to interact with and use AI safely.

It is pivotal to understand that there is a distinction between human interaction and machine-generated responses; seemingly human-like performances can create false security. Here are some best practices:

1. **Critical Thinking:** Treat AI responses with skepticism; make sure to double check any statements and verify the information with 2-3 sources. AI often produces incorrect or fictitious information.
2. **Online Safety:** Make sure to never share personal information like your name, address, hometown, school or phone number with AI tools or chatbots.
3. **Report Inappropriate Content:** If you encounter offensive or inappropriate interactions, report it to the platform, service provider, or a trusted individual.
4. **Decision Making:** Don't overly rely on AI for decision-making, especially for schoolwork or work assignments. It could be considered plagiarism or cheating.

Sources:

https://www.defendyoungminds.com/post/ai-safety-for-kids-6-best-practices-every-parent-should-know

https://kpmg.com/xx/en/our-insights/ai-and-technology/eight-tips-for-using-ai-safely.

Cybersecurity Resources for Kids

We have pulled together some of the best cybersecurity resources available for kids of every age to keep them entertained, educated and safe while they spend time online.

- Be Internet Awesome with Google - Interland is an online game that helps kids learn the importance of digital safety. Through the games, children will combat hackers, phisers and bullies by practicing the skills needed to be good digital citizens.

- Carnegie Cyber Academy provides a gamified learning experience for children. Participants are invited to take on the role of cadets and take part in training missions that teach them how to safely engage in internet activity.

- FBI's Safe Online Surfing has entertaining games and teacher resources to keep children of all ages safe online.

- Kids Safe Online Activity Book - The Center for Internet Security (CIS) created an activity book for children to learn key cybersecurity terms and common cybersecurity threats through interactive puzzles, word searches, coloring pages and quizzes.

- **Public Broadcasting Service (PBS)** has interactive quizzes, games and a library of resources to educate children, parents and teachers about cybersecurity.

  Visit: https://www.pbs.org/wgbh/nova/labs/lab/cyber/ *-and-* https://pbskids.org/cyberchase/

YOUR CYBERSECURITY COMMUNITY AWAITS YOU

Join WiCyS... where the recruitment, retention and advancement of women in cybersecurity HAPPENS!

For more information, email us at info@wicys.org

WICYS.ORG