CTC Information Technology Division Annual Cybersecurity Bulletin

OCTOBER 2024

October is National Cybersecurity Awareness Month!

Topics/Quick Links

CENTRAL TEXAS COLLEGE®

CYBERSECURITY AWARENESS MONTH

"Secure Our World" is the Cybersecurity & Infrastructure Security Agency (CISA)'s theme for this year's Cybersecurity Awareness Month 2024. This theme focuses on helping people, businesses, and families stay safe online, and is broken down into the following four steps:

- Recognize & Report Phishing
- Use Strong Passwords
- Turn on MFA
- Update Software

A toolkit for this year's Cybersecurity Awareness Month is available for free and can be used year around to increase cybersecurity awareness.

WHAT THE IT HELP DESK WILL AND WILL NOT ASK YOU

When the IT Help Desk sends you an email, how do you know it's really them?

Keep the following tips and points in mind the next time the IT Help Desk sends you message:

- The IT Help Desk will **NEVER** ask you to change your password in an email or text message.
  - The IT Help Desk **WILL** assist you in changing your password, but only if you call or message the Help Desk first!

- The IT Help Desk will ALWAYS use the following email addresses:
  - HDesk@ctcd.edu
  - Help.Desk@ctcd.edu

- An email from an official IT Help Desk Technician will always end with a signature that contains their name, contact information, and the official CTC logo.

WHAT THE IT HELP DESK WILL AND WILL NOT ASK YOU CONTINUED...

The IT Help Desk will **NEVER** ask you the following, under any circumstance:

- Your password
- Your social security number
- Your home address
- Your credit card or banking information

The IT Help Desk **WILL** ask for the following information after you have reached out to them for assistance:

- Name
- School ID Number
- Email Address
- Phone Number

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial Intelligence, commonly referred to as AI, has been all the craze of 2024. AI is a field of science concerned with building computers/programs that can reason, learn, and act in such a way that would normally require human intelligence. AI systems learn and improve through exposure to vast amounts of data and by identifying patterns and relationships in this data. Algorithms (sets of rules or instructions) guide the AI's analysis and decision-making.

WHAT CAN ARTIFICIAL INTELLIGENCE DO?

AI can be used for speech recognition, image recognition, translation, predictive modeling, data analytics, and cybersecurity.

- Automation - AI can automate workflows and processes, such as verifying documents, transcribing phone calls, or answering simple questions from customers on an organization's chat bot.
- Reduce Human Error - AI can eliminate manual errors in data processing, analytics, and other task through automations and algorithms that follow the same processes every single time.
- Eliminate Repetitive Tasks - AI can be used to perform repetitive tasks, freeing people to work on high-level problems.
- Infinite Availability - AI can be "always on" and continuously working on its assigned tasks.
- Accelerated Research and Development - AI has the ability to analyze vast amounts of data quickly, which can lead to accelerated breakthroughs in research and development.

THE HAZARDS OF USING AI

Users and organizations alike should be aware of the ethical, legal, security issues that come with using AI.

- Security Risks - Malicious actors can harness the power of AI to develop more advanced cyberattacks, bypass security measures, and exploit vulnerabilities in systems.
- Deepfake Creation - Cybercriminals are using easily accessible AI tools and data to mimic people's voices and images (referred to as "deepfakes") to make fake calls and videos. Deepfakes are used to harass, blackmail, and threaten individuals for monetary, political, and influential gain.
- Privacy Concerns - AI systems often collect and analyze large amounts of personal data, raising issues related to data privacy and security.
- Bias and Discrimination - AI systems can inadvertently perpetuate or amplify societal biases due to biased training data or design of its algorithm.
- Ethical Dilemmas - Instilling moral and ethical values in AI systems presents a considerable challenge. Researchers and developers must prioritize the ethical implications of AI technologies to avoid negative societal impacts.
- Legal and Regulatory Challenges – Legal frameworks and regulations have not been enacted yet to meet the unique issues created by the use of AI that we are now seeing. It will most likely take several years for the legal system to catch up.
- Misinformation and Manipulation - AI-generated content contributes to the spread of false information and the manipulation of public opinion.

CTC AI TOOL SAFETY

To mitigate privacy risks, we must advocate strict data protection regulation and safe data handling practices. The IT Division provides the following recommendations for using AI tools safely.

- CTC faculty and staff have access to Microsoft Copilot. Copilot is Microsoft's ChatGPT-powered interface that can be accessed through Bing search, the Microsoft Edge browser, Windows 11, a downloadable app, and directly at the Copilot website.
- Before using Copilot, you will need to sign in with your CTC / Office 365 login information.
- With Copilot, you can schedule meetings, set reminders, create to-do lists, transcribe meetings, and summarize long articles. It can also assist you with research, writing, editing, and generating ideas.
- Copilot provides enterprise-grade security and privacy when a CTC user is logged in. Information entered into Copilot will not be shared outside of the protected session, nor will it be retained or used to further train the underlying AI.
- Due to this protection and security, the IT Division recommends that CTC users only use Copilot or other AI tools available through approved enterprise applications that CTC licenses (e.g., BlackBoard Ultra).

CTC AI USE GUIDELINES

The IT Division asks that users abide by the following guidelines when using *Copilot* or *BlackBoard Ultra*:

- **Protect confidential data**: Do not upload or share any data that is confidential, proprietary, or protected by regulation. This includes data related to students, faculty, or staff.
- **Control access to accounts**: Do not share login credentials or other sensitive information.
- **Comply with security policies**: Apply the same security best practices we use for all company and customer data.
- **Keep information private**: Exercise discretion when sharing information. Employees should always keep the following questions in mind before uploading or sharing any data into an AI tool:
  - Would I be comfortable sharing this information outside of the College?
  - Would the College be okay with this information being leaked publicly?

Likewise, don't forget to brush up on the procedures and regulations set in both the **CTCD HR Policy 294: Computer Security Policy and the CTCD HR Policy 295: Computer Usage!**

WATCH OUT FOR THESE SCAMS—EMAIL SCAMS

It's important to be cautious with unsolicited emails, especially those that prompt you to click on a link or download an attachment. Always check the sender info of any email, and never share sensitive information unless you're certain of the recipient's authenticity and can encrypt/secure the information that needs to be shared. If you're unsure, contact the IT Help Desk.

Fake Email Receipts
This a type of phishing scam where scammers send emails that appear to be purchase confirmations or receipts from legitimate companies. These emails often contain links or attachments that, when clicked or opened, can install malware on your device or lead you to a fraudulent website designed to steal your personal information.

Fake Password Reset Emails
These types of emails appear as warning from Microsoft, the IT Help Desk, your email provider, or any software company. They often advise that you need to change your password (or other account information) ASAP, or you might suffer from some sort of consequence (e.g., email account being locked, loss of messages, inability to use the software in question).

Fake Antivirus Software Emails
These emails appear as advertisements (or warnings that you are unprotected) for fake antivirus software. You are often encouraged (or threatened) to pay for and download (or update) the software, which will most likely contain some form of malware (e.g., trojan, tracker, worm, etc.).

WATCH OUT FOR THESE SCAMS—PHONE SCAMS

Phone scams have only gotten more numerous and more sinister this year, and this trend does not appear to be letting up any time soon. Remember to never share personal information over the phone with unknown callers, and always verify the identity of the caller through official channels. Let unknown calls go to voicemail on your personal phones, and never trust caller ID as it can be spoofed.

Phone Call Phishing (Vishing)
The term 'vishing' is a portmanteau of the words 'voice' and 'phishing'. As you can already assume, this tactic is used by malicious actors to extract personal information via a phone call. If you think you've become the target of a vishing attempt, hang up the phone immediately! Do not give the scammer any further information about yourself or Central Texas College. The following vishing attempts have been reported to the IT Division this year:

WATCH OUT FOR THESE SCAMS—PHONE SCAMS CONTINUED...

- ***"Updating CTC's Google listing" Scam***
  Be wary of anyone claiming to be a representative of Google. As stated on Google's "Help protect against fraudulent calls" page, "Google will never ask you for payment information over the phone or guarantee you favorable placement in our products."

- ***"Can you hear me?" Scam***
  Scammers record your voice when you answer various questions to use for authorizing fraudulent charges or services in your name. Always be cautious of unsolicited calls, and avoid confirming any personal information that may be brought up in a conversation.

QR Code Phishing (Quishing)

QR codes are easy to make, easy to share, and easy to use, but they are also very easy to exploit. Be cautious of random QR codes on webpages, emails, or printed on flyers/posters. While these codes are often used as glorified weblinks, they can also be used to direct unsuspecting users to malicious websites (where malware can automatically be downloaded or your private information can be harvested). Do not trust every QR code you come across. Only scan codes from people or institutions that you absolutely trust!

MFA Push Notification Spamming

This scam, also known as multifactor authentication (MFA) fatigue, has been hitting schools, hospitals, and businesses more frequently (as more institutions are now implementing MFA). Malicious actors flood a user's device with MFA push notifications in order to confuse a user and trick them into approving a fraudulent login attempt. This then grants the scammer access to the target's account. Never approve a random MFA request. If you receive multiple MFA requests, ignore them or contact the IT Help Desk.

Cybersecurity Double Puzzle

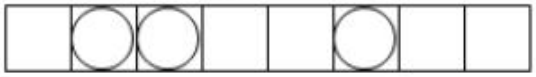
CYBERSECURITY AWARENESS MONTH

SECURE OUR WORLD

Double Puzzle

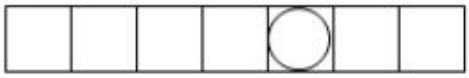
Solve the anagrams and use the circled letters in the top part to complete the final phrase at the bottom. Each circled letter is used just once.

AOSDRPWS 

TNRETENI 

UTDPEA 

YRISTCEU 

PYRICAV 

PECTOMUR 

AEKCHR 

EEICVD 

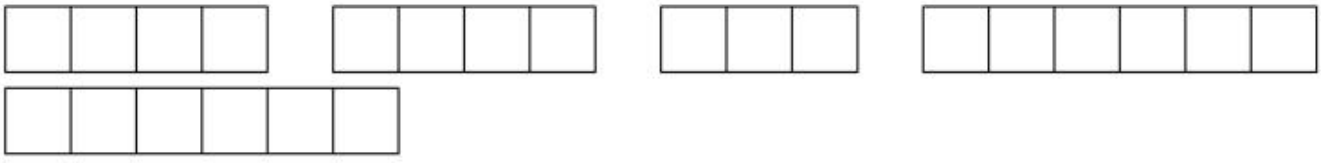
IWIF 

RCEBY 

IRYFEV 

ELARMWA 

GOILN 



Find the Cyber Terms!

CYBERSECURITY AWARENESS MONTH

SECURE OUR WORLD

Find the Cyber Terms!

E V W X U P D A T E L O R P
I N T E R N E T D F O V I S
N B H A C K E R T I G V X R
O E R J M X E K B R I W W A
V O T E C Y F J X E N N K N
I O U W A F Y K I W G D D S
R L P V O C P B Y A E D A O
U U O A R R H V K L N A N M
S W R G S E K J Q L C T A W
M T T U S S M W H K R A H A
D V S J E O W A W J Y T D R
C O O K I E S O I F P E T E
E G U P H I S H R L T J K Z
T M A L W A R E A D T P S U

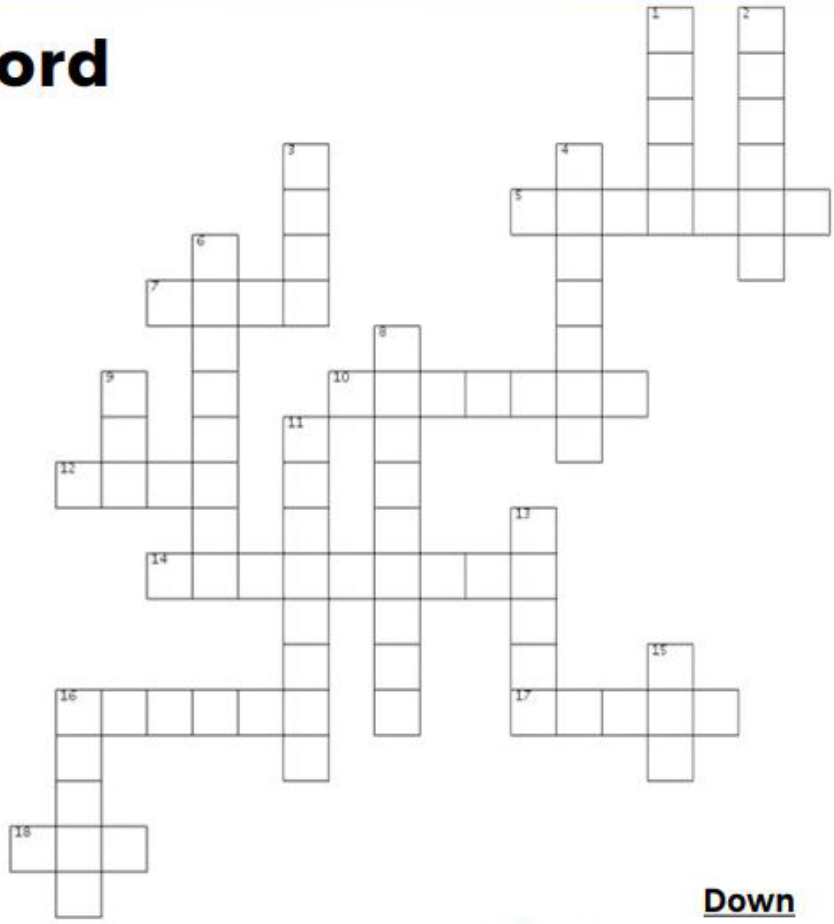
Update
Cookies
Encrypt
Email
Internet
Password
Phish
Malware
Data
Hacker
Virus
Network
Ransomware
Login
Firewall

Cybersecurity Crossword

CYBERSECURITY AWARENESS MONTH

SECURE OUR WORLD

Crossword



Across

5. Spoofing is when bad actors create a fake _____ and send phish emails to imitate a business.

7. If you receive a suspicious _____ hover over it with your mouse before clicking to make sure it is real!

10. Bad software installed on a computer to damage or harm it. Examples are viruses, Ransomware, Spyware, etcetera.

12. A _____ breach is when a hacker successfully breaks into a system and exposes private information.

14. Wireless short-range connection for devices in the same network. Phones, computers etcetera.

16. A piece of data about your online history that creates a trail of crumbs. Not chocolate chip, though.

17. _____ colon forward slash forward slash before a link website U R L means it is encrypted and secure.

18. A big surprise problem in your computer. Sometimes it is small like an ant or big like a cricket.

Down

1. Malware that infects a computer by corrupting or erasing information and sending it to hackers.

2. Always _____ your devices and software when the newest version is available!

3. When a cybercriminal tries to take your information by sneaking into your computer.

4. When multiple devices are connected together to share information, they are together in a _____.

6. Any tech used to keep bad actors out. It burns the hackers.

8. Always use long and unique _____ for each of your online accounts.

9. This sends an email or text when logging in to make sure it is really you.

11. The online network we use to share information around the world. You use it everyday.

13. When a hacker pretends to be a real person to fool you into clicking on a fake link or file. Usually an email or text message.

15. Private network to make you anonymous on the internet.

16. Global network for servers to share and store information. It doesn't rain from the sky though!

And Remember!

- The IT Security webpage has a tech tip section, a tech terms cheat sheet for tech jargon, and offers easy access to all IT related policies for CTC.
- If you're looking for an encryption tool or password manager for your CTC computer or laptop, the IT Division recommends Encryption Wizard and KeePass. Both can be found on the IT Hardwar/Software page. Guides are also available via the IT Security Tech Tips page.
- **When in Doubt, Contact the IT Help Desk!** If you believe your CTC workstation may be compromised, or if you are concerned about a strange email, please contact the IT Help Desk at #3103 or via email at help.desk@ctcd.edu.
- Don't forget to brush up on the procedures and regulations set in both the **CTCD HR Policy 294: Computer Security Policy and the CTCD HR Policy 295: Computer Usage!**
- Here are the answers to the above puzzles.