CTC Information Technology Division Annual Cybersecurity Bulletin

OCTOBER 2025

OCTOBER IS NATIONAL CYBERSECURITY AWARENESS MONTH!

TOPICS/QUICK LINKS

CENTRAL TEXAS COLLEGE

CYBERSECURITY AWARENESS MONTH

Stay Safe Online – The Core 4
This year's theme, Stay Safe Online, is all about the simple ways to protect yourself, your family and your business from online threats. Small actions can make a big difference.

That's why we're focusing on **the Core 4**. Four easy steps anyone can take to boost their online safety:

- Use strong passwords, a password manager, and MFA
- Recognize and report scams
- Update your software
- Back up your data

USE STRONG PASSWORDS, A PASSWORD MANAGER, AND MULTIFACTOR AUTHENTICATION

Passwords play a central role in maintaining security. Current standards state that a longer, more difficult password to guess is stronger than a password that is constantly changed on a schedule. And while it is good to have a strong password that never expires, it can be difficult to remember a passphrase that is:

- Over 14 characters long
- Unique (not used for any other login)
- Made up of a mix of uppercase letters, lowercase letters, and numbers

Likewise, entering it correctly into multiple applications that are needed for everyday work can be both frustrating and tedious.

This is where a password manager can help. A password manager is an application that can be used to store your login information. Many password mangers also come with a password generator, which can be used to make difficult passwords for you. Information stored in a password manager is often encrypted and locked behind a password. (This means, you will only have to remember one password for logging into your computer, and one password to access all your stored passwords on your password manger.) Password mangers are a fantastic way to both keep your login information safe and to save time.

The IT Division recommends KeePass for anyone looking for a new password manager. KeePass is a free and open source, desktop-based password manger that also comes with its own password generator. You can download KeePass from https://keepass.info/.

USE STRONG PASSWORDS, A PASSWORD MANAGER, AND MULTIFACTOR AUTHENTICATION CONTINUED...

Multifactor Authentication (MFA) is an additional security feature that requires users to verify their identity. This is often done by having the user type in and/or approve a code that is sent via email, text, or in an app.

According to the Cybersecurity and Infrastructure Security Agency (CISA) and Microsoft, multifactor authentication (MFA) can block up to 99% of automated hacking attempts. If MFA is available, it is best to always enable it.

Typical MFA methods include:

- An additional password
- A code sent to your phone, email, or app
- A fingerprint or facial scan

RECOGNIZE AND REPORT SCAMS

Recognizing Email Scams

Email scams are becoming increasingly sophisticated, making it essential to stay vigilant. Here are key signs to watch for and tips to protect yourself:

Common Red Flags

- Urgent Requests: Messages that pressure you to act fast, like changing your password or confirming account details, are often scams.
- Spoofed Senders: Emails that appear to come from trusted sources (e.g., Microsoft, your IT Help Desk, or your bank), but use fake email addresses, signatures, or logos.
- Fake Antivirus Alerts: Prompts to download or pay for antivirus software.
- Generic Greetings: Be cautious of emails that start with "Dear Customer" instead of using your name.
- Suspicious Links or Attachments: These can direct you to phishing sites or install malicious software on your device.

RECOGNIZE AND REPORT SCAMS CONTINUED...

What You Can Do

- Never click on links or download attachments from unknown senders.
- Always verify the sender's information before taking any action. Verify the sender's email address and look for official signatures.
- Never share sensitive information unless you're completely certain of the recipient's identity.
- When in doubt, contact the IT Help Desk for guidance.
- Staying informed and cautious is your best defense against email scams.

Recognizing Phone Scams (Vishing)

Just like with email scams, phone scams are designed to trick you into giving away sensitive information or approving unauthorized access. Stay alert by watching for these common tactics.

Common Vishing Tactics

- Impersonation: Scammers may pose as anyone (e.g., a family member, a Google rep, tech support) to ask for personal details or scare you into paying for something.
- Caller ID Spoofing: A familiar-looking number doesn't guarantee legitimacy. Scammers will often fake caller IDs, and they can make their call look like it came from your bank or your boss.
- MFA Fatigue Attacks: Attackers may flood your device with multifactor authentication requests, hoping you'll approve one out of frustration or confusion.

What You Can Do

- If possible, let unknown calls go to voicemail. It is easier to assess a message in voicemail than it is to deal with a practiced scammer's story or threats in real time.
- Never share personal information over the phone unless you initiated the call and trust the recipient.
- Hang up immediately if the caller pressures or threatens you, or if they request sensitive data.
- Stay calm, cautious, and informed. If you ever feel unsure of something, 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.

Does Making a Report to the IT Help Desk Help?

Yes, we have blocked over 600 phishing email addresses locally in the past 5 years. Our phishing emails are forwarded to the Texas Department of Information Resources (TX DIR) for analysis. This information is then used to help block malicious downloads and phishing campaigns state-wide. TX DIR shares information with state agencies (including other institutions of higher education) weekly to block malicious IP addresses and domains. To date, CTC is blocking almost 25,000 malicious domains and over 9,200 malicious IP addresses at the firewall.

Many thanks to our reporting regulars for helping us keep CTC safe!

UPDATE YOUR SOFTWARE

Keeping your software up-to-date is one of the best ways to protect your devices from malware and online threats. Make sure that you are always running the latest version of your operating system (like Windows), app, browser, or antivirus program.

Why it matters: Software updates often include critical security patches that fix the vulnerabilities exploited by malware and hackers.

What you can do:

- Enable automatic updates whenever possible.
- Don't wait to install available patches.
- Regularly check for updates
- Remove unused programs or add-ons as they can become entry points for cyber threats.

A few minutes of updating now can save you from hours of recovery later!

UPDATE YOUR CTC WORK COMPUTER DRIVERS

A driver is a program that enables your computer to communicate with a hardware device (e.g., a monitor, a printer, graphics card, keyboard, or mouse). When drivers are not installed correctly or updated regularly, hardware devices may not function properly. To manually update your CTC work computer's divers:

1. Click on the Microsoft Shield icon (formally the Start button).
2. Open Settings.
3. Select Window Updates from the bottom of the left column.
4. Open the Advanced options menu.
5. Select Optional updates.
6. From here, check all of the boxes for programs/software that need to be updated. There may be multiple drivers that need to be updated, as well as available Windows updates. Click the Download & Install button after you have selected everything available.
7. Wait for updates to install. Then, restart your computer after updates are completed or when prompted.

BACK UP YOUR DATA

Remember to keep current backups! If you happen to become a victim of ransomware, having a working, up-to-date backup can save you the trouble of having to start completely over. The IT Division recommends requesting and using a network share folder to backup files that do NOT contain personally identifiable information (PII).

Data Governance
Data Security

Safety	Storage Location	PII/Sensitive Data OK?	Reliably Backed Up
Most Safe	Colleague and Softdocs	✓	✓
	Network Share	X	✓
	CTC Workstation	X	X
	Laptops	X	X
Least Safe	USB drives, removable drives, mobile devices, etc.	X	X

SOPHOS EMAIL PROTECTION

On Friday, August 8, CTC implemented Sophos Email Protection. All incoming and outgoing email messages to and from the @ctcd.edu domain are now routed through Sophos' email security system. This upgrade is designed to significantly reduce the number of malicious emails received by CTC.

As we continue to fine-tune the process, some legitimate emails may be mistakenly quarantined. Be sure to carefully review any messages from Sophos regarding quarantined emails. If you need a group or sender whitelisted, please contact the IT Help Desk.

While this added layer of protection will help minimize spam and harmful messages, it is not foolproof. If a message seems unusual in any way, be cautious, and contact the IT Help Desk.

THE DOWNSIDES OF AI

While AI tools boost productivity, users need to keep in mind the risks.

- Privacy & Security: AI systems need lots of data, which can lead to leaks, unauthorized access, or exposure of personal info. Entering PII into AI tools is strictly forbidden by CTC.
- Cyber Threats: AI can be misused to create deepfakes, phishing scams, and malware.
- Legal Uncertainty: Laws haven't caught up with AI, creating confusion around accountability and compliance.
- Bias & Ethics: AI may reflect biased data, leading to unfair decisions and reduced human interaction.
- Dependency: AI can cause overreliance and reduce critical thinking.

NEW AI TOOLS POLICY

A new AI policy has been created that outlines the requirements that users must follow when using AI tools, including the evaluation of security risks and the protection of confidential data. All CTC users are expected to adhere to the following security best practices when using AI tools:

- Protection of confidential data: Users must not upload or share any data that is confidential, proprietary, or protected by regulation. This includes data related to students, faculty, or staff. CTC users must exercise discretion when sharing information publicly.

- Access control: Employees must not give access to AI tools outside the college, and subsequent processes as required to meet security compliance requirements without prior approval from the CTC Information Security Officer. This includes sharing login credentials or other sensitive information with third parties.

- Use of reputable AI tools: Users should use only reputable AI tools and be cautious when using tools developed by individuals or companies without established reputations. Any AI tool used by CTC users must meet CTC security and data protection standards.

- You can read the new policy in full via the IT Security webpage.

- Please contact the IT Help Desk if you have questions about using a particular AI-based tool.

WHY THE IT DIVISION ENDORSES COPILOT

The IT Division recommends using Microsoft Copilot due to its enterprise-grade security, its privacy protections, and its compliance with institutional policies. Copilot ensures that:

- Data entered during a session is not shared externally, not retained, and not used to train the AI.
- Sessions are protected when users are logged in with their CTC / Office 365 credentials.

AND REMEMBER!

- **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!**

CYBERSECURITY WORD SEARCH

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

Hidden Words

- **Antivirus**
- **Bluetooth**
- **Cybersecurity**
- **Encryption**
- **Firewall**
- **Hacker**
- **Malware**
- **Network**
- **Passphrase**
- **Password**
- **Phishing**
- **Ransomware**
- **Smishing**
- **Trojan**
- **Vishing**
- **Vulnerability**