CTC Information Technology Division
Annual Security Bulletin

FALL
2023

October is National Cyber Security Awareness Month!

Creating a Culture of Cybersecurity Awareness at Central Texas College

Texas Administrative Code 202 (TAC202) requires that employees of state agencies and higher education receive cybersecurity awareness training annually. At CTC, we meet this requirement by conducting cybersecurity training every April and reinforce our training with the IT Cybersecurity Newsletter in October. But cybersecurity awareness is more than just meeting state requirements – it needs to be part of our day-to-day work culture too. Our cybersecurity culture should encourage us to recognize threats, curb poor online behavior, and follow basic security habits on a daily basis.

Cybercriminals know that people are the weakest link in any cybersecurity ecosystem. Seventy-four percent of all breaches worldwide include the human element. Ninety percent of cyberattacks start with a phishing email. Yet, most employees believe they know how to recognize a phishing email. However, according to the Verizon 2023 Data Breach Investigations Report, 30 percent of all phishing emails are opened, and links are clicked 12 percent of the time. Nine out of 10 ransomware infections come from some form of phishing event. It doesn't matter how many cybersecurity resources an organization has if the users don't think about cybersecurity when engaging with technology.

Ordinary users are on the frontline of the cybersecurity war, constantly being bombarded by malware, phishing, and other scams. Policies and procedures are important tools that help protect an organization's important data, but a successful cybersecurity culture (one that entails creating a mindset that cybersecurity risk is real and that our daily actions impact that risk) really is the secret weapon that can help turn the tide.

CENTRAL TEXAS COLLEGE®

How to Create a Culture of Cybersecurity

Creating a culture of cybersecurity requires a comprehensive approach that includes policies, procedures, and training. Here's what any organization can do to create an effective culture of cybersecurity:

1. **Develop a comprehensive cybersecurity policy**: A cybersecurity policy is a set of guidelines that outlines how CTC will protect its data and systems. This policy should cover everything from password management to network access to data backup and recovery.

2. **Communicate the cybersecurity policy to all employees**: Once the policy is developed, it is essential to communicate it to everyone. This can be done through employee training sessions, email communications, or college-wide meetings.

3. **Train employees on cybersecurity best practices**: In addition to communicating the policy, it is essential to provide training on cybersecurity best practices. This can include training on how to identify and report potential security risks, how to create strong passwords, and how to avoid phishing scams.

4. **Implement security controls**: Security controls are measures that an organization can implement to protect data and systems. This can include firewalls, antivirus software, intrusion detection systems, and access controls.

5. **Regularly review and update the policy**: Cybersecurity threats are constantly evolving, so it is essential to regularly review and update the cybersecurity policy to ensure it is up-to-date with the latest threats and best practices.

6. **Lead by example**: Creating a culture of cybersecurity requires leadership to lead by example. Executives and managers should follow the same cybersecurity policies and procedures as all other employees and ensure they enforce these policies in their respective teams.

7. **Encourage reporting**: It is crucial for everyone to feel comfortable reporting any potential security risks or incidents. This can include reporting phishing emails, suspicious activity on the network, or any other potential security threat. To encourage reporting, an organization should provide clear channels for employees to report incidents and ensure that employees are not punished for reporting potential security risks.

8. **Perform regular security assessments**: These assessments (such as VAPT – Vulnerability and Penetration Testing) are used to identify and address potential vulnerabilities before they are exploited. Security assessments should be tailored to fit an organization's needs and may include penetration testing, vulnerability scanning, and risk assessments.

9. **Celebrate successes**: When employees identify and report potential security risks or incidents, it is important to acknowledge their successes.

Fact: Cyber-attacks occur about every 39 seconds, and most of them (95%) are due to human error. Promoting a culture of proactive security and collective responsibility within our organization can help reduce risks and protect our data.

Remember to review HR policies 294 & 295 on Computer Security and Computer Usage!

The Risks and Rewards of Using AI in the Workplace

There is a lot of talk about AI and ChatGPT these days, but what exactly are they? How are they being used in the workplace? And are they a new threat or a helpful tool?

Artificial intelligence (AI) systems are simply computer systems and programs that have been designed to complete a job or task. Here at CTC, an AI system you may already be familiar with is our IVY chatbot (EagleBot). EagleBot assists the IT Help Desk (and other departments utilizing it) by answering many of our user's easier questions online. This, in turn, gives our Help Desk employees more time to answer phone calls and handle more difficult issues. The IVY chatbot is a generative chatbot powered entirely by organization-specific data and Generative Pre-trained Transformer 3 (GPT-3). You may have also heard of another very popular AI used for chatting that also uses GPT – ChatGPT. GPT is used to "humanize" information. Our IVY chatbot uses GPT to turn the data it has been given into replies and answers that are easier to read and understand.

Using AI in the workplace can offer numerous benefits, such as automating tasks, improving efficiency, and providing quick access to information. However, there are potential dangers and challenges associated with the use of AI in a professional setting that users will need to keep in mind. If you currently use or plan to use AI in some manner in the workplace, please be aware of the following risks:

1. **Bias and Fairness**: AI systems can inherit biases present in the data they are trained on, leading to discriminatory outcomes. In a workplace context, this can result in biased decision-making, hiring practices, performance evaluations, or unfair treatment of employees. For instance, using AI to assess employee productivity may not account for individual circumstances or unique contributions. If AI is brought into any of the above processes, it will need to be strictly monitored and scrutinized.

2. **Privacy Concerns**: You should never enter private or sensitive information into an AI system – especially one owned by a third party. Doing so may expose yourself or CTC to cybersecurity risks, such as data breaches, leaks, or unauthorized access by bad actors. (Doing so also goes against CTC security policy.)

3. **Overreliance on AI**: An overreliance on AI for decision-making or problem-solving can lead to complacency among employees, who may stop critically evaluating outcomes or actively participating in decision-making processes.

4. **Upkeep**: While AI has a reputation for freeing up time, a huge time investment is often needed to get AI programs up and going. Likewise, AI systems need to be updated and maintained continuously.

5. **Quality Assurance**: Maintaining the quality of AI-generated content can be challenging, especially at places like CTC (and higher education institutions in general) where there are always new students, new events, and new changes every semester. Poorly generated or incorrect content can harm an organization's reputation if it is not kept in check.

6. **Technical Failures**: AI systems can experience technical glitches or errors (like any and all technology), which can disrupt workflows, customer service, or decision-making processes if not managed effectively. Be prepared, and have a backup plan just in case.

The Risks and Rewards of Using AI in the Workplace Cont...

To mitigate these dangers, organizations and users should carefully consider the ethical, legal, and practical implications of using AI in the workplace. Implementing robust policies, conducting regular audits, ensuring transparency in AI decision-making processes, and providing ongoing training for employees are some ways to address these challenges.

All CTC users are expected to adhere to the following security best practices when using AI tools:

All CTC users are expected to adhere to the following security best practices when using AI tools:

1. **Evaluation of AI tools**: Users must evaluate the security of any AI tool before using it. This includes reviewing the tool's security features, terms of service, and privacy policy. Employees must also check the reputation of the tool developer and any third-party services used by the tool.

2. **Protection of confidential data**: Users cannot upload or share any data that is confidential, proprietary, or protected by regulation without prior approval from the CTC Information Technology Division. This includes data related to students, faculty, or staff.

3. **Access control**: Employees cannot share login credentials or other sensitive information with AI tools outside the College or other third parties. If an exemption to this rule is required, approval from the CTC Information Security Officer or Chief Technology Officer must be received first.

4. **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.

5. **Compliance with security policies**: Employees must apply the same security best practices we use for all company and customer data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies.

6. **Data privacy**: CTC users must exercise discretion when sharing information publicly. 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 made public?

For Your Information

- 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.
- StaySafeOnline promotes cybersecurity and privacy education and awareness. Learn how to protect yourself, your family, your workplace, and your devices with their tips and resources.
- If you would like to ask the CTC EagleBot a question, just click on the blue, speech-bubble icon at the bottom-right corner of any webpage where the bot has been placed.

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.
- **The IT Division/IT Help Desk will NEVER ask for your login information!** We will never email you about changing your password. Neither the IT Division nor Sophos will ever distribute an update or software fix through email.

Further Research

Remember, cybersecurity is everyone's responsibility, and creating an effective cybersecurity culture requires a collective effort. Here are a few helpful links if you are interested in further research:

- State of Texas Administrative Code
- Implementing a Cybersecurity Culture
- Why Build a Cybersecurity Culture?
- Phishing Facts
- What is a Culture of Cybersecurity?