

# CyberSafe Holidays

## November 6, 2024

The holiday season is generally a time to relax and reconnect with family and friends.

Cybercriminals also love the holiday season – they see it as the perfect time to take advantage of you, and attacks skyrocket. Phishing for example, increases by more than 150 percent (above average) according to Barracuda.

During the holiday season, it is important to be extra vigilant when shopping, giving, or booking travel plans. Don't let cybercriminals steal your holiday fun! Keep the following in mind to better protect your personal information.

## Shopping Online

- **Use secure Wi-Fi.** Using free Wi-Fi to shop online, at your favorite coffee shop is convenient but is not cybersafe. Use a VPN (virtual private network) or your phone as a hotspot to shop.
- **Lock down your login.** Create a long and unique passphrase for all your accounts, and use multi-factor authentication (MFA) when possible.
- **Resist the urge.** Be wary of offers too good to be true – no matter how tempting. Only buy from trusted and established online retailers.
- **Think before you click.** Pay attention to emails you receive. Don't open emails from unknown senders or click on links in suspicious messages.
- **Shop securely.** Make sure you are shopping on a protected site (using SSL – secure sockets layer). This encrypts the data between a website and a browser. The easiest way to know is to look at the URL in the browser's address bar – look for an **s** in **https** (http is not secure).
- **Pay wisely.** Use a credit card or pre-paid debit card, instead of a debit card linked to your bank account. Or, use a reliable, established third-party payment service (e.g. Google or Apply Pay).
- **Monitor your accounts.** Check your online financial accounts regularly for suspicious spending. Take advantage of text and email alerting services many banks and credit card companies offer.

## Giving Online

- **Do your research.** Never feel pressure to give on the spot. Visit the IRS website to learn what types of organizations can get tax-deductible donations. Learn about charities and

how they spend the money they receive.

- **Ignore unsolicited requests.** Be wary of emails and phone calls asking for donations, especially organizations unfamiliar to you. Instead, visit their website directly or call to donate.
- **Think before you pay.** Never wire money or send cash. Pay by credit card; or, if donating online, make sure the website is secure by looking for the **https** at the beginning of the URL.
- **Double check the website.** Check the URL carefully – cybercriminals often create fake websites very similar to the real organization. Check the spelling of the organization’s name for discrepancies.

## Traveling

- **Disable auto-connect on your devices.** If your mobile phone or tablet automatically connect to wireless networks or Bluetooth devices, disable those features. When you want to connect, do so manually.
- **Secure your device.** Keep track of your laptop, smartphone, tablet, and even accessories, such as USB (universal serial bus) drives.
- **Avoid shared computers.** If using computers at hotel business centers or other places, with shared systems, avoid making purchases or logging into email. You do not know if the systems are up to date with the latest security software or if the machines are safe.

## MCC Cyber Team Wins 1<sup>st</sup> Place

We would also like congratulate the MCC Cyber Team for winning 1<sup>st</sup> place in the [Cybersecurity Interdisciplinary Incident Response Competition \(CIIRC\)](#)! MCC competed against Baylor University (2<sup>nd</sup> place) and Texas A&M University (3<sup>rd</sup> place) at the Cyber Range, as part of the Central Texas Cyber Initiative (CTCI).

CIIRC was a three-day, student competition to simulate real world events occurring in business. The competition scenario simulated a business environment suffering cyber-attacks. Teams had to identify and analyze the attacks, determine and address recovery, public consequences, financial ramifications, engage in a press conference, report to the U.S. Securities and Exchange Commission (SEC) according to regulations, and many other related activities.

In the debrief, the Baylor staff administering the competition offered many complementary remarks about the MCC team and were very impressed with their performance. This demonstrates the caliber of our students, faculty, and administration. This is an example of who we send out into the world.

---

Revision #1

Created 12 December 2024 18:57:05 by Laura J. Crapps

Updated 12 December 2024 18:58:43 by Laura J. Crapps