# A Message From

THE INFORMATION SECURITY TEAM

**This communication is intended for all Modivcare team members.** If you are unsure whether this message applies to you or have additional questions, please contact us at questions@modivcare.com.

## Holiday scams are here. Are you prepared?

We want everyone at Modivcare to celebrate and be safe this holiday season.

While you celebrate, please be aware that cybercriminals are also going above and beyond their normal tricks to steal your personal information, such as passwords and payment details.


**Here are some common holiday scams, along with tips to keep you safe and prepared.**

## Charity Scams

Cybercriminals know that Thanksgiving, Hanukkah, Christmas, Kwanzaa, and New Year's are peak donation times; that's why they create sneaky scams to exploit your generosity.

- Beware of suspicious emails and websites.
- Visit Charitynavigator.org to understand where your money is going.
- Pay with a credit card whenever possible and avoid cash donations, which are harder to trace.

## Travel Scams

Are you thinking about hopping on a plane this year? Here are three scams to watch out for:

Phishing emails from booking sites – Did you book your trip online? Beware of phishing emails. Make sure emails that require clicks are legitimate, and not a pesky scammer impersonating a booking site.

- Never provide your banking details or transfer money.
- Navigate back to the source site or application to confirm any issues.

- Always book from reputable sites with customer reviews, support, and a secure URL (look for the green lock icon in your browser).

Juice jacking – Did you know that criminals can replace USB ports with malware-infected cables that steal your data while your phone charges?

- Don't use a public USB port to charge your phone (keep a portable power bank handy if you have one).
- Traditional power outlets are safer than USB charging stations.
- You can also connect your device to a USB data blocker, which allows charging, but blocks any data transfer.

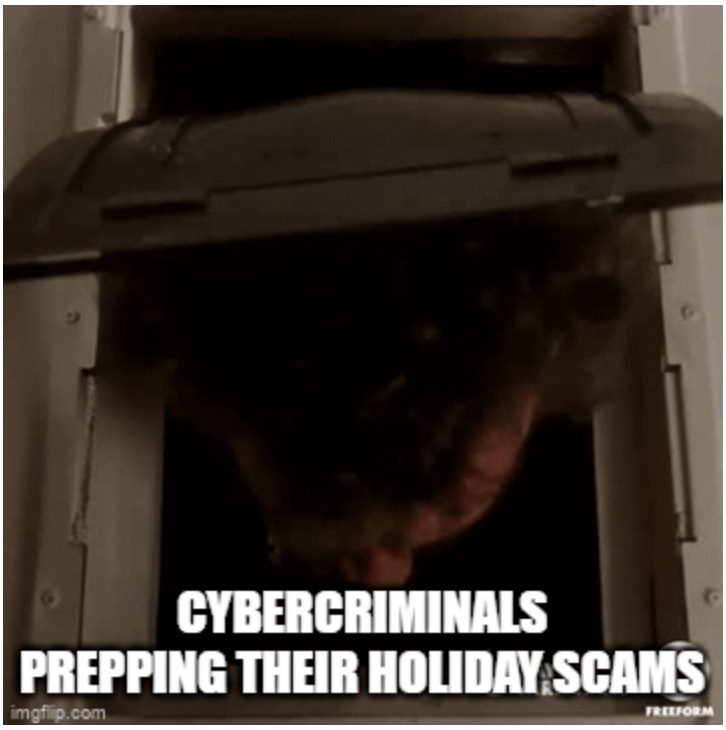
Fake Wi-Fi hubs – Hackers can create unsecured public Wi-Fi hotspots in common areas and access your passwords, online accounts, etc., on that fake Wi-Fi network.

- To avoid fake Wi-Fi hubs, always check with the coffee shop, hotel, or restaurant for their official network connection.
- Even better, use your own hotspot if you have one.

### Shopping Scams

It's no secret that shopping ramps up during the holidays, but scams do too. Be careful about how and where you share information and beware of fraudulent retailers and organizations.

- Protect your information and make purchases only on secure networks.
- Always pay by credit card and keep receipts for refunds.




***Words of Wisdom***

*“Stay safe and use these tips to enjoy the holidays with peace of mind.”*

Securely yours,

The Information Security Team