
# UTHSC G.U.A.R.D.

Holiday 2019

IN THIS ISSUE

## *Gift Card Scams: Our Campus and Beyond*

***by Chris Madeksho, Information Security Analyst***

A quarterly report from Agari, an information security email solutions company, reports that while cybercriminal organizations have numerous options for cashing in on their successful scams, the gift card had become the king of cash-outs. Gift cards were requested in over half of all BEC (business email compromise) scams in the third quarter of 2019.

So why try a gift card scam? The scam starts with a simple email spoofing the name of someone with authority in an organization. The email can be sent to numerous people at the same time. If the phish gets hooked, and thinks they are doing a favor for a coworker or friend, the payoff can come quick.

The average cost of a gift card scam is $1,571. On our campus, based on what has been reported to ITS, the average cost to the individual has been about $500. While we are attempting to stop these emails from even getting into everyone's inbox, the bad actors are getting more and more clever in the delivery of these emails. So, yes, people are still falling for it. Google Play is the most requested gift card in these scams, but others, such as Steam Wallet, Apple iTunes and retailers such as Amazon, Walmart and eBay have also been reported.

You can help by reporting any suspicious email to abuse@uthsc.edu. We can examine the email and take steps from stopping the attack to our campus. For more information, contact IT Security at 901.448.1880 or itsecurity@uthsc.edu.


### *Gift Card Scams?*

*These scams are still on campus this season!*

### *Shopping Tips*

*Learn some best practices when shopping online and in store*

# *Shopping Tips for the Holiday Season*

***by Thomas F. Duffy, MS-ISAC Chair***

It's that time of year again, holiday shopping has begun! Everyone is looking for those unique gifts, hot toys and cool electronics. While it's clear that businesses are after your dollars during the holidays, you should be aware that cybercriminals are on the lookout, too.

When it comes to holiday shopping, you need to be careful that you don't fall prey to these criminals. Here are some tips to following for your holiday shopping:

**Online Shopping**

1. Do not use public Wi-Fi for any shopping activity. Public Wi-Fi networks can be very dangerous, especially during the holiday season. Public Wi-Fi can potentially grant hackers' access to your usernames, passwords, texts and emails.
2. Look for the lock symbol on websites. The lock may appear in the URL bar, or elsewhere in your browser.
3. Know what the product should cost. If the deal is too good to be true, then it may be a scam.
4. Keep your computer secure. When using your computer to do your holiday shopping, remember to keep your Anti-virus software up to date and apply all software patches. Never save usernames, passwords or credit card information in your browser and periodically clear your offline content, cookies and history.

**In-Store Shopping**

5. Always us credit cards for purchases. Avoid using your ATM or debit card while shopping. In the event that your debit card is compromised, criminals can have direct access to the funds from your bank account.
6. Don't leave purchases in the car unattended.
7. Beware of "porch pirates". Consider having your holiday packages delivered to a family member, your workplace, or a trusted neighbor.

For more information, contact the Information Security Team at itsecurity@uthsc.edu or 901.448-1880.