Here are four of this season's top cyber threats, according to cybersecurity experts:

1. Black Friday/Cyber Monday Specials

Scammers often advertise big-ticket items to lure unsuspecting consumers to click on links. Bad guys build complete copies of well-known sites, send emails promoting great deals, sell products and take credit card information – but never deliver the goods.

"Sites that seemingly have unbelievable discounts should be a red flag. When something is too good to be true, it likely is," Ondrej Krehel, founder/CEO of the New York City-based cybersecurity intelligence firm LIFARS, said. "These sites look like legitimate stores, but use these web fronts to collect sensitive information, including credit card numbers."

2. Free Vouchers or Gift Cards

A common Internet scam involves big discounts on gift cards. These sites usually request enough personal information for criminals to raid victims' bank accounts.

Social media site posts also offer phony vouchers or gift cards, with some being paired with holiday promotions or contests. Some posts may even appear to have been shared by a victim's friend. Often, these posts lead to online surveys designed to steal personal information.

In August 2015, a link began circulating on Facebook that promised users a $100 JCPenney coupon in exchange for liking and sharing a post. Users who clicked through those shared links reached a page titled, "Back to School with a $100 JCPenney Coupon." However, the URL was "JCPeeney.net," not JCPenney.com – the department store's official website.

3. Ransomware, DDoS and Site Overload

Last July, the Internet Crime Complaint Center issued an alert regarding an increasing number of complaints from businesses hit by distributed denial of service extortion campaigns via email. In a typical extortion campaign, the targeted business receives an email threatening a DDoS attack on the company's website unless it pays a ransom.

DDoS attacks result in damaging consequences, including lowered customer confidence and lost revenue. The attack might not be large enough to crash a website, but it's just large enough to get noticed. The attack is then followed by an email claiming responsibility and threatening a bigger attack if the ransom isn't paid.

During site overloads, sites receive more traffic than they can handle, overwhelming it and potentially causing it to crash. According to Neustar, 88% of consumers distrust websites that crash.

4. Phishing on the Dark Side

A new email has begun circulating that tricks people into thinking they could win movie tickets for the highly-anticipated film, "Star Wars: The Force Awakens," due out on Dec. 18. However, the email is a phishing attack in disguise.

Sjouwerman cautioned that leading up to the film's release, this will be highly successful social engineering attack that a lot of users are going to fall for.