SCAMS ARE BREWING

A look at the tactics cybercriminals are using this holiday season

THIS MONTH'S TOPICS:

Grab your favorite drink and settle in while we spill this month's cyber tea!

As you take on holiday shopping with your warm brew in hand, remember, cybercriminals have new scams brewing too. Don't let your online shopping or holiday social media posting grind to a halt because of these scams.

In this month's newsletter, learn about the tactics circulating social media and online shopping platforms. By the time you finish this newsletter, you will be ready to take on the digital holiday season armed with a big cup of solid cyber habits.

3 Social Media Threats

Phishy Buyers

Online selling platforms and social media marketplaces can make it easy to connect with buyers for your old items. But scammers don't only pose as sellers. Be wary of buyers who:

- Ask to move the conversation to another platform.
- Overpay for an item unprompted.
- Ask for your personal information.
- Don't have a profile picture or profile information.

Bait-and-switch Posts

Scammers are making attention-grabbing posts about missing children or injured animals, urging users to share them to spread the word. After users have reposted the message, the scammer switches it to show a link to a survey that "guarantees cash prizes" or a fake ad for a rental property. Since this still shows up on the user's page as a repost, many of their online friends might think they are recommending the link. If interacted with, these ads often lead to malware or identity theft. To avoid playing a role in these scams, look into the person doing the original posting, do a reverse image search, and check if the supposed news has been reported by other outlets before reposting.

Fake Employee Discounts

Scammers are posting to social media pretending to be ex-employees of a store. They claim to be "seeking revenge" on their previous employer by offering their employee discount to followers. They claim the discount gets you items for free; you just have to pay for shipping. Once an order is placed, the website disappears, or they refuse refunds. Users are left with no item or a cheap knockoff. If a post seems phishy, report it to the social media platform.

Holiday Edition

ONLINE SHOPPING

DEALS AND DISCOUNTS

Especially around the holidays, it can be difficult to identify the real sales from the phony ones. The best way to do this is to stick to deals and discounts offered by reputable companies. If a deal is real, it should be announced on the official website.

RETURNS AND REFUNDS

Check the store or item policy for returns and refunds before purchasing. One sign of a scam is a website that does not offer returns or refunds or does not outline their policies clearly anywhere.

HOLIDAY SHOPPING TIPS

1. Avoid buying presents through suggested social media ads before researching.

2. Always research and read reviews before buying from a new company.

3. Shop with a credit card since they offer more help with fraudulent charges.

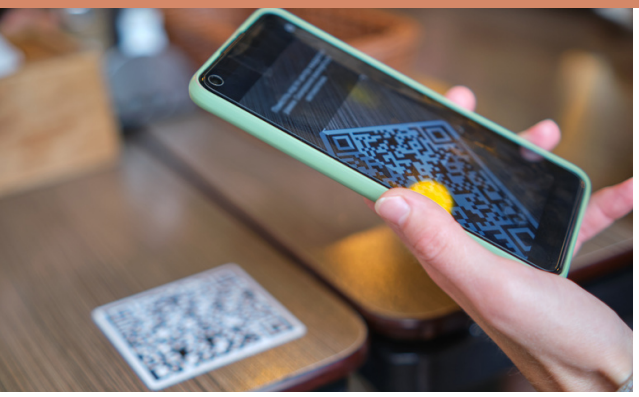
4. Limit the personal information that you share with a website to only that which is necessary for the purchase, and don't save card details.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

As the holidays approached, Ed planned to meet some family and friends out for dinner. When the day finally came, he drove to the restaurant and parked his car in a lot nearby. Ed walked over to the pay station and noticed it had a QR code on the side of it that said, “Scan & Park”. Ed examined the machine. It looked old and had some buttons missing. He decided it would be easier to scan the QR code and pay for the parking digitally.

After entering his card details, email address, and phone number, he waited for a confirmation message. But the message never came. Eager to get to dinner, Ed shrugged it off and continued on his way to the restaurant. The night went swimmingly until Ed walked back to his car after the dinner. Not only did he have a parking ticket, but when he went back to the website from the QR code and examined it closely, he realized it didn’t have any details related to an official parking company.

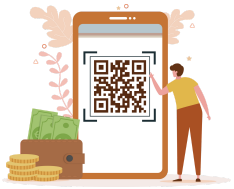


Did you spot the red flags?

- Ed should have examined the website before entering his personal information.
- Since the pay station was functional, Ed could have paid directly through this more legitimate source, even if it took a little more time.
- If Ed looked at the QR code closely, he would have seen it didn’t have a company name or other sign of legitimacy.

QR codes can be made by anyone and stickers can be placed in public settings. Avoid scanning random QR codes before verifying the source.

Be wary of QR codes placed randomly on pay stations, especially if they don’t state any details about the website or company involved.



Some cybercriminals stick their malicious QR code over legitimate ones. Even if the sticker is from a well-known company, examine it closely for any signs of tampering.

THE MONTHLY MASHUP

KEY TAKEAWAYS

The holidays are a time cybercriminals try to take advantage of. Whether you are shopping online, or scrolling on social media, be sure to think twice before clicking this time of year.

JOKE OF THE MONTH

Why did the computer catch a cold during the holiday season?

Because it left its Windows open while browsing for presents!

NOVEMBER 30TH: COMPUTER SECURITY DAY

This holiday was created to remind us to take the time to consider if our computers and personal data are as secure as they can be.

SOCIAL MEDIA CHALLENGE

Which social media post is most likely a scam?

1.

2.

Answer: Post 1