STAY SECURE WHILE YOU SCROLL

Lock down your chats and avoid social media mishaps

THIS MONTH'S TOPICS:

If you thought losing hours due to mindless scrolling was the worst thing that could happen on social media, think again. Scammers are using social media platforms and messaging apps to carry out scams where they steal your money or personal information.

In this month's newsletter, learn how to spot social media and messaging app scams. From enticing advertisements that ask for too much information to urgent requests from a friend in need, we've got the scoop on how to spot these social scams. We will also look at how AirDrop and other short distance sharing features could be used by cybercriminals.

Social Media Scams

ScamAlert

Cybercriminals use social media platforms to carry out many different scams. They hack real profiles to message the person's friends, advertise fake products or pose as celebrities. Follow the tips below to make sure you stay secure while scrolling.

StaySecure

Social Media Tips:

- Avoid sending money to friends you meet online, even if they claim they need it for an emergency situation.
- If you receive an out-of-character message from a friend, don't click on any links. Message the person via another form of contact first.
- Avoid buying things from social media ads. Research the company first and then go directly to their official website.

CHAT APPS

Scammers are utilizing chat apps to carry out their scams. Don't respond to unknown, unsolicited chats.

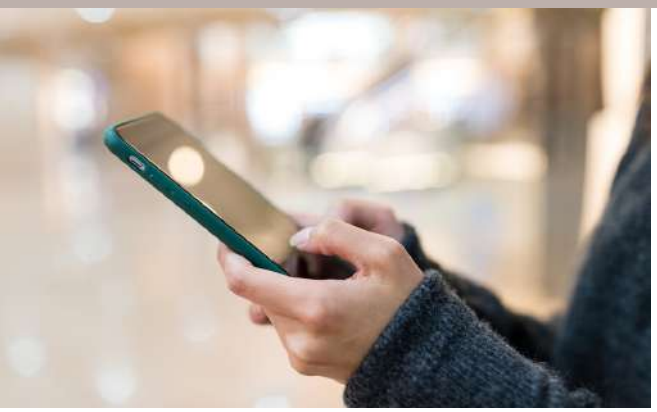
SCAM OF THE MONTH

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

Carrie lives in the city and often finds herself in crowded places such as subways and airports. She passes the time traveling by scrolling on her phone.

One day, Carrie was on a bus when a notification popped up on her phone. It was an AirDrop requesting to send her a file. Carrie didn't realize she had her share settings open to everyone. She didn't know the sender but out of curiosity, she accepted the file.

The file was nothing special. It had data related to a company Carrie was not familiar with. She clicked around on the file, and it opened a strange link. Carrie closed out of the file and the link and assumed it was sent to her by mistake. But really, it carried malware that worked its way through her device. Over the next few days, her phone began to behave erratically, with apps crashing and battery life draining unusually fast. Carrie ignored the signs, assuming she just needed a new phone.



Did you spot the red flags?

- Carrie should have had AirDrop turned off when not in use or set to private. Some use AirDrop to send inappropriate photos or malicious files.
- When Carrie started noticing her phone acting erratically, she should have scanned her device with a trusted antivirus app.

AirDrop has had issues in the past with vulnerabilities, allowing cybercriminals to see a user's phone number or email address. Keep devices updated to make sure any security vulnerabilities are patched as soon as possible.

AirDrop on Apple devices and Nearby Share on Android devices let users send pictures or files without an internet connection. They use Bluetooth and create a peer-to-peer Wi-Fi network. Keep these sharing features private or off when not in use, and only accept files from trusted contacts.

CYBER NEWS

JUNE
2024

FTC RELEASES NEW LIST OF MOST IMPERSONATED COMPANIES

According to a recent report by the FTC, Best Buy/Geek Squad, Amazon, PayPal, and Microsoft were among the most reported impersonated companies last year. While Best Buy/Geek Squad was the most frequently reported, the most money lost occurred in Microsoft-related scams. Other organizations with a high number of reports and losses include Wells Fargo, Norton, and Apple. This report is a reminder to verify the sender or caller of any unsolicited interactions by checking the organization's official email or phone number, even when you recognize the organization's name.

UPDATES & EVENTS

Some celebrated Internet Safety Month in June. Even once June is over, continue the celebrations by making sure you have security settings in place and sharing tips with others.

HACKERS TARGET CLOUD APPS

Some hackers are stealing sensitive data from cloud applications. One way they do this is by reaching out to a company's help desk, claiming they are an employee who needs help resetting their password or MFA. The group then uses legitimate tools within cloud environments to extract data. For those who reply to help desk requests, it is crucial to verify the identity of the person submitting the request. All employees should limit who they let access their cloud and what they store on the cloud when possible. It is also important to implement MFA in every place possible.