LIGHTS, CAMERA, SCAMS!

How cybercriminals capitalize on the entertainment industry

THIS MONTH'S TOPICS:

Celebrity Scams

How cybercriminals use celebrities...

Entertainment Scams

The topics that get users to click...

Scam of the Month:

Celebrity Endorsement Scams...

The Monthly Mashup:

May Updates and Review...

We are all drawn to entertainment. Whether it's watching your sports team in an exciting game, streaming the new episode of a popular show, or watching your favorite singer perform live, there is something out there for everyone.

But as we let our guards down, ready to relax into a good story, cybercriminals are ready to pounce.

In this month's newsletter, learn more about how cybercriminals use different forms of entertainment to carry out scams and cyberattacks.

CELEBRITY SCAMS

ENDORSEMENT SCAMS

From fake skincare lines to investment platforms, or even charity donations, the types of fake celebrity endorsements are endless. Before purchasing, research the product and check the celebrity's social media account to see if they mention the partnership. But, be sure to use caution with links posted to the celebrity's real social media account. Cybercriminals will try to hack these accounts and push their fake websites in order to steal users' data and money. It is best to go directly to a legitimate website to make these transactions, rather than follow a link.

AI VOICE AND VIDEO SCAMS

With the rise of artificial intelligence and deepfakes, scammers are making fake voice recordings and videos of celebrities to advertise their products or create shocking clickbait online.

SOCIAL MEDIA SCAMS

Scammers often create fake social media accounts to carry out scams, as well. They may use a familiar celebrity to do this. Check if an account is verified and look at the number of followers on the account before following. If you receive a message from a celebrity out of the blue, asking you for money or to click on a link, it is likely a scam.

CELEBRITY SCAM TIPS

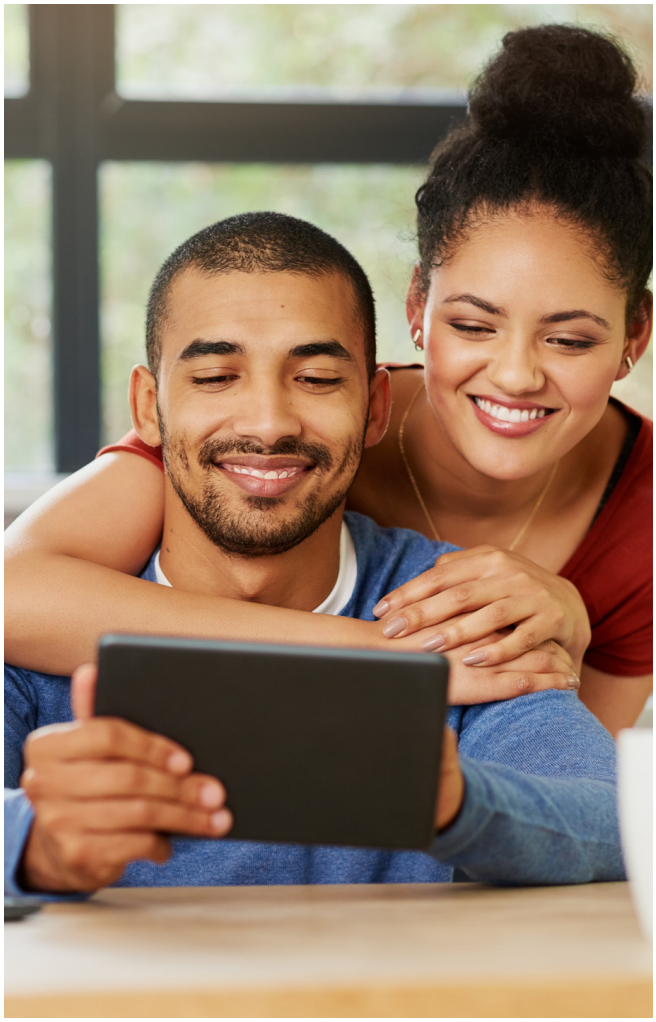
- Proceed with caution if you receive a message from a celebrity.
- Research products before buying, even if they are endorsed.
- Analyze celebrity videos or audio for robotic cadence or odd facial movements.

If celebrity content seems out of character, don't interact with it, as this is a sign of a scam.

Entertainment Scams and Techniques

Engagement and Entertainment Scams

Users are more likely to engage with topics they are familiar with or interested in. Let's go over the ways cybercriminals take advantage of this by using these topics to carry out scams.



Clickbait Content

Cybercriminals create dramatic fake news as clickbait. This could be celebrity gossip or stories about serious world events. AI-generated articles only help to increase the amount of content that can be pushed out. For emails containing this type of content, use the SLAM method to analyze the sender, links, attachments, and messaging. For websites, stick to news from trusted sources and look for the "lock" symbol.

Entertainment Content

Many types of entertainment like streaming platforms, sports events, or online contests may be used as bait in phishing messages. It is always best to go directly to a company's website instead of clicking on links in emails.

Event ticket scams are on the rise, as well. Try to buy tickets from the original seller and avoid buying through ads. Whether it is a ticket, a jersey, or a streaming platform, if the price seems too good to be true, it probably is.

Entertainment Applications

Cybercriminals have taken to app stores to create replicas of popular entertainment applications. This could be streaming apps, popular games, or music platforms.

While third-party app stores are the most susceptible to these malicious apps, it is always best to check the number of reviews and the developer before downloading an app. If a malicious app is downloaded, it could infect a device with malware and allow the cybercriminal to access user data.

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.

Rachel was looking for a new skincare product. She started searching the web and saw an ad for a skincare cream used by one of her favorite singers. Rachel was excited, she had just been to her concert and thought this skincare cream must be great if the singer was endorsing it. Rachel clicked on the ad and was taken to the company's website where she was greeted with more pictures of their products and other celebrities that had tried them.

She selected a cream and continued to checkout. After a few weeks, Rachel still hadn't received the cream. She started to get suspicious and tried to find a confirmation email. Rachel realized she never received a confirmation.

When she performed an internet search on the brand, she found many reviews from other customers saying it was a scam. When Rachel checked her credit card, she found multiple fraudulent charges. Luckily, she was able to call her credit card company and get the money back.

Did you spot the red flags?

- Rachel trusted the company because of the celebrity endorsement and did not research the company first before buying the product.
- Instead of staying on well-known websites, Rachel clicked on an ad to buy the product.
- Rachel did not receive a confirmation email for her order, and did not check her credit card transactions until weeks later.

Check the celebrity's social media account to see if they have posted anything about endorsing the product.

Take the time to investigate the company before buying anything. Always use a credit card when making new purchases online.

With the rise of deepfake videos and AI voice generation, celebrity endorsement scams are getting more complex. If a product is unknown but endorsed by a celebrity, it is best to conduct further research before purchasing.

THE MONTHLY MASHUP

KEY TAKEAWAYS

There are many ways cybercriminals capitalize on the entertainment industry. Even if a headline or deal speaks to your interests or curiosity, it is still best to proceed with caution.

JOKE OF THE MONTH

What do hackers use to phish?

Clickbait!

MAY 26TH: PAPER AIRPLANE DAY

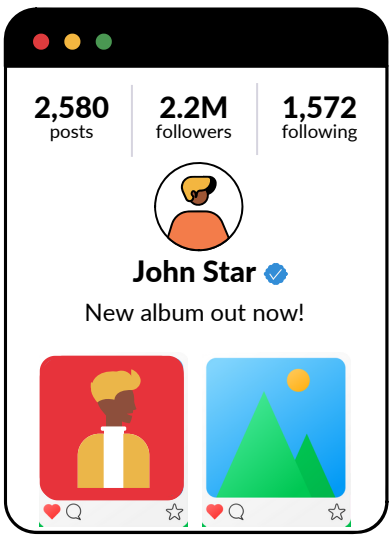
Follow these steps to celebrate:

1. Make a paper airplane.
2. Write down a cybersecurity tip on it.
3. Let your cyber-tip fly!

SPOT THE FAKE

1.

2.



Answer: Number 1 is the fake.