TRENDING: CURRENT EVENTS AND SCAMS

How cybercriminals are bringing the heat with hot topics

THIS MONTH'S TOPICS:

If there is a current event, you can be sure a scam is running rampant! Shocking headlines about hot topics often catch our attention more than a typical piece of online content, and cybercriminals are capitalizing on that notion by creating scams related to these events. From election news to significant legislative changes, political milestones often serve as fertile ground for sophisticated scams. Fake and real emergencies and natural disasters are also used to draw users' attention.

In this month's newsletter, explore examples of current event scams, and how cybercriminals are using natural disasters, health emergencies, and global crises, to make their scams more convincing.

Current Event Scams

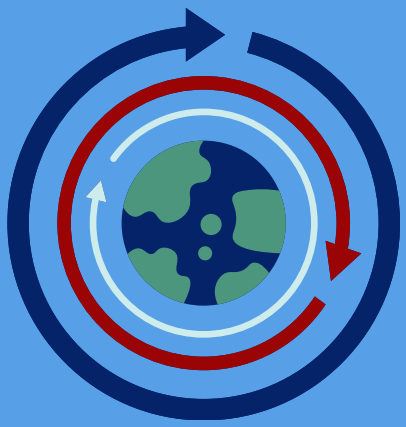
Political events, such as elections or governmental transitions, are prime times for cybercriminals to launch targeted scams. Scams may include misinformation campaigns, fake fundraising for political causes, or phishing attacks disguised as urgent political updates.

News and Deepfakes

The rise of audio and video deepfakes has made it even easier for scammers to spread misinformation. Just because you see a video, audio recording, or picture of someone doing something shocking online, doesn't mean it really happened.

26%

of users surveyed were confident in their ability to spot fake news.



Phishing Messages

Using the guise of political surveys, polls, campaign updates, or donation requests, scammers send messages to trick individuals into providing personal information or clicking on malicious links.

EMERGENCY SCAMS

Emergency-related scams take many forms, from fake charity donation requests to fraudulent emergency relief. These scams leverage the urgency and emotional weight of events to bypass rational scrutiny and provoke immediate action.

Health Emergency

During health crises, scams often surface involving products claiming to prevent or cure diseases.

- Consumers should be wary of products that make broad health claims.
- Fake news and testimonials are also used by scammers in relation to health emergencies.

Natural Disaster

In the aftermath of natural disasters, scammers often impersonate authorities or create fake charities to exploit the public's desire to help.

- Watch out for third-party sales of emergency supplies that are sold out elsewhere.
- Verify charities or organizations before donating.

Global Crisis

Global crises, like economic downturns or geopolitical conflicts, can lead to an increase in scams. Fear based headlines are used as well as deals promising high returns to alleviate financial insecurity.

- Verify shocking headlines through a trusted news source.
- Be cautious of any offer that seems too good to be true.

Scammers will also try to spread misinformation about fake events or emergencies. Always consult with trusted sources or professionals before making decisions, especially during times of crisis when emotions might cloud judgment.

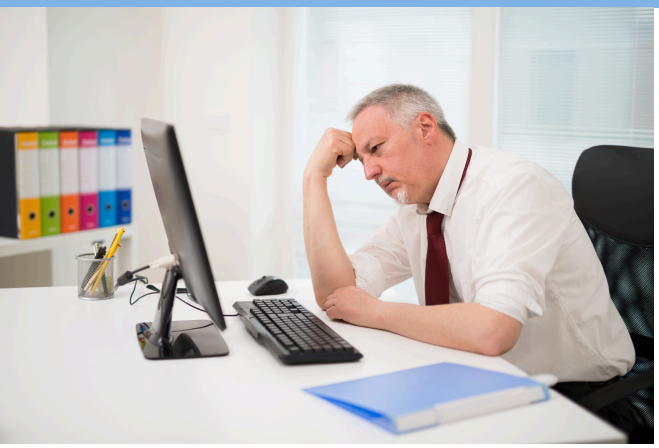
SCAM OF THE MONTH

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

Max enjoys staying up to date with economic and business news. One morning, as Max scanned news stories online, a breaking headline popped up about a severe economic crash. The article was detailed and convincing, citing unnamed experts and confidential reports. It painted a grim picture of the days ahead, advising readers to divest from certain stocks and invest heavily in others it claimed were recession-proof.

Driven by a mix of fear and the opportunity to outmaneuver the market, Max made the decision to adjust his portfolio accordingly, redirecting significant funds into the recommended assets.

Days turned into weeks, and the predicted economic catastrophe failed to materialize. It was only then that the truth dawned on him – he had followed the advice of a fake news article designed to manipulate the market or get unsuspecting users to click on certain malicious links.



Did you spot the red flags?

- Max should have verified the news through other sources before making decisions based on one article.
- Instead of scanning news stories online from random websites, Max should have specifically gone to the websites of credible news outlets that he trusted.
- Max should have paused before acting on emotions fueled by something he saw online.

Many headlines (real and fake) related to current events use emotionally charged language or shocking details to get the user to click a link or stay on their site. It is important to be aware of this. Take a step back and think twice before acting on a headline.

Some cybercriminals create fake news websites that resemble the design, name, and URL of real news websites. It is important to scrutinize websites and URLs before interacting with a site or clicking on links.

CYBER NEWS

MAY
2024

MALICIOUS COMMENTS

A case was discovered where cybercriminals hid malicious code within an image on a comment to a product website. The hidden code aimed to steal consumers' data by bypassing security measures. While this specific case was discovered and thwarted by a threat management system, it is important that users are careful when interacting with images in comments and reviews. Organizations should make sure to employ continuous web threat management solutions to detect and prevent such vulnerabilities.

UPDATES & EVENTS

There are many holidays and elections coming up. As you enjoy these holidays and navigate the elections, remember to be on the watch for holiday scams and fake headlines.

FAKE TOLL ROAD TEXT MESSAGES

Scammers are trying to trick drivers into paying fake toll fees with this new scam. They send text messages impersonating toll collection services, claiming that the recipient owes money for unpaid tolls. The message often includes a link to a fake website that appears legitimate. If financial information is entered on the fake website, it could lead to identity theft and financial loss. Always verify toll payment requests through official websites, or by contacting the company's customer service directly, instead of clicking on unsolicited links.