SecurityAwarenessNews

the security awareness newsletter for security aware people

The Age of Disinformation:
How Social Media Threatens Security

Misinformation and Disinformation

Social Media Security

How to Spot Fake News

©2021 The Security Awareness Company - KnowBe4, Inc. All rights reserved.

Misinformation and Disinformation

We live in a world where news spreads faster than ever and our daily lives are shared in real time. But what happens when the news is maliciously tampered with and the facts we consume are exposed as untrue? Let's explore these challenges of social media, starting with two important definitions:

- **Disinformation:** *false information that is intentionally created and disseminated to deceive people.*
- **Misinformation:** *false information that is inadvertently spread by misinformed individuals.*

The difference between the two comes down to intent. Disinformation is deliberately spread, while misinformation is often spread by people who are tricked into believing false stories.

Which one is more dangerous?

Disinformation sounds more insidious than misinformation, but they are equally dangerous. No matter how bad information spreads, the net impact harms all of us.

Why would anyone want to create and spread false information?

Disinformation campaigns have many intentions. In some cases, they're used to sow doubt, create division, interfere with political issues, or ruin reputations. In other cases, fake headlines are used to generate clicks and website activity in hopes that digital advertisers will buy space. In almost every scenario, false information intends to deceive and maliciously shape public opinions.

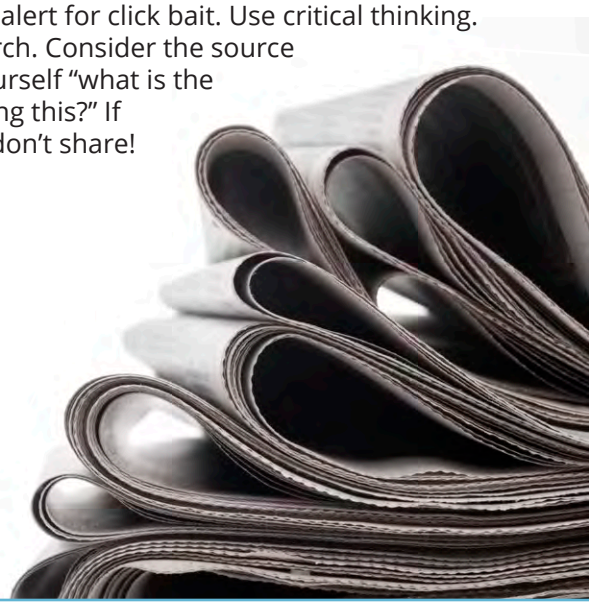
How do disinformation campaigns harm organizations and individuals?

Imagine if someone crafted a fake story about a popular car manufacturer, claiming that their vehicles randomly explode after a certain amount of mileage. If this story hits the right news cycle, it could permanently ruin the manufacturer's reputation, destroy their market value, and potentially lead to bankruptcy.

On a personal level, bad information can put strain on relationships with friends and family. And as we've seen too many times in too many countries, these campaigns sometimes lead to violence.

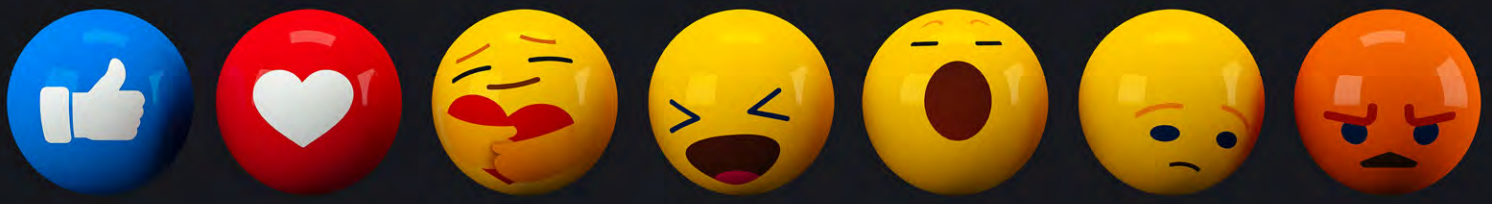
What can we do to stop disinformation and misinformation?

Remember that you have a lot of control over what you see on social media and, more importantly, what you share. Stay alert for click bait. Use critical thinking. Do some research. Consider the source and think to yourself "what is the benefit of sharing this?" If you're unsure, don't share!



© 2021 The Security Awareness Company - KnowBe4, Inc. All rights reserved.

Social Media Security



Before getting into how to use social media responsibly and securely, we need to first realize an unfortunate truth: there is no such thing as 100% privacy. When you set up an account on a social media platform, you are entrusting that platform with your personal information. It's your responsibility to find out how your data might be used, and if the platform you intend to join can be trusted. (And be sure to protect your accounts with strong, unique passwords!)

With that in mind, let's review a few ways scammers use social media and how we can stay safe while still enjoying all of the benefits these platforms offer.

Data Mining

People tend to overshare without considering the risks, which provides a great resource for scammers who collect personal data and use it to launch targeted phishing campaigns. For example, a cybercriminal may search social media to discover your job title, your place of employment, your top interests, what social groups and networking communities you join. They then use this information to create scams or phishing emails that appear legitimate. Avoid this by setting accounts to private and thoroughly vetting all friend requests. Even then, never share anything confidential or offensive.

Fake Profiles

Fake profiles come in a variety of forms. Bots, short for "computer robots," can perform automated tasks that mimic human interactions and generate comments, likes, shares, and other actions to spread disinformation or create division.

Scammers also set up fraudulent accounts that impersonate people you know, with the intention of gaining access to all of the data previously mentioned, along with your entire network of friends, family, and co-workers.

Phishing Attacks

Not only do cybercriminals spread malicious links via popular social media apps, they also craft phishing emails that mimic real sites. It's easy to steal logos and other recognizable features that help trick people into thinking the message is real. Think before you click, and report all phishing attacks immediately.

Deepfakes

Deepfakes are media sources like audio files, videos, and pictures that have been manipulated by technology to appear to be something they are not. The more the technology improves, the harder it becomes to identify deepfakes. As a general rule, if something sounds or looks unbelievable, assume that it's fake.

Beyond scammers, social media can lead to negative impacts on your personal and professional life. A seemingly innocent post could be misinterpreted, go viral, and result in someone getting fired or banned from various forums. So always consider the consequences of your actions before posting. Here at work, follow our organizational policies regarding social media, and if you have questions, please ask.

© 2021 The Security Awareness Company - KnowBe4, Inc. All rights reserved.

How to Spot Fake News

Thought Exercise

Which of the following statements are fake?

"Elon Musk sells his Tesla shares to focus on a new cryptocurrency venture."
"Pope Francis arrested for fraud."
"Shark seen swimming on a flooded highway after Hurricane Harvey."
"Coronavirus can be cured by drinking a bowl of boiled garlic water."
"Airplane that disappeared mid-flight 37 years ago reappears and lands without incident."

If you guessed that all of the above are fake, you guessed right. Each qualifies as fake news. Worse yet, they were circulated and widely engaged with by millions of people. And even though some fake statements cause little harm, we've witnessed many that result in public confusion, destruction of reputations, and sometimes violence. No matter how dangerous or frivolous, all forms of fake news carry real consequences. You can spot them by following these tips:

Consider the source:

Most fake news is generated by random, untrustworthy news sources that have no credibility. When you see a headline making a strong or unbelievable claim, research the source before reacting or sharing.

Check for references:

If a news story contains no cited sources or references, it's likely fake. Almost every honorable journalist and media outlet provides links that credit the original source of information. Of course, the cited sources could themselves be fake. So, once again, critical thinking is vital.

Research the author:

Try to find the answers to these questions: Who wrote the story? What other stories have they authored? Do they seem heavily biased? Who's sharing it? Has it been picked up by multiple news outlets?

Learn to be objective:

It's impossible not to have some level of bias towards things like politics, entertainment, sports, and so on. But it's important to ignore those biases in favor of searching out the truth in headlines. People are likely to believe a fake story is true when it caters to their own beliefs and principles.

What does this have to do with cybersecurity?

It's easy to dismiss fake news as a problem for social media platforms and not necessarily a problem for data protection. But cybercriminals use fake news to drive people to malicious websites that distribute malware. We witnessed this issue explode during the pandemic, when corrupt sites sold fake cures that were intended to defraud people and spread malware.

That reinforces why it's so important to use social media responsibly. Not only does spreading bad information hurt society, a careless click could also result in personal data or money being stolen. So just like you do with all cyber threats, use common sense, think before you click, and if you don't know if something is real, don't share it.

© 2021 The Security Awareness Company - KnowBe4, Inc. All rights reserved.