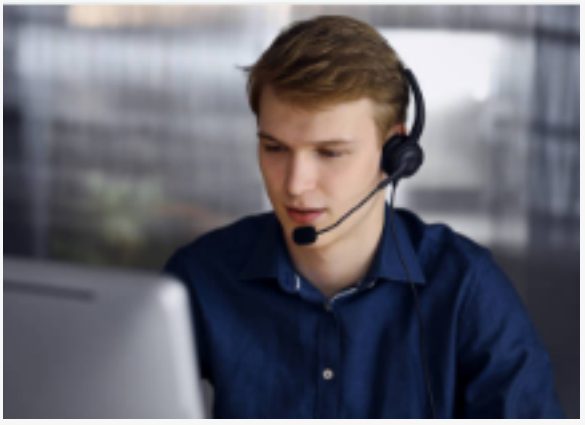
Fake Twitter emails might contain malicious attachments: Cyber-Forensics.net explains why they are dangerous.

Scammers are creating fake emails to look like they are from Twitter. These fake emails contain malicious attachments to steal financial data.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, March 10, 2022 /EINPresswire.com/ -- Social Media platforms like WhatsApp, Facebook, and Twitter have become an integral part of human communication. These platforms are places where a considerable number of audiences are readily available. This audience is often looking for opportunities to connect with a wide range of communities sharing the same interests.

But scammers are running a new kind of scam and taking advantage of this curiosity. This time, they are using Twitter to vandalize consumer privacy.

The cyber thugs create fake emails that resemble emails sent by Twitter. But the twist is. Unlike Twitter which sends informative emails, these fake emails contain harmful attachments. The scammers are doing this by manipulating a few symbols and icons here and there and sending spyware to attack their target's financial data.

Cyber-Forensics.net, a cyber forensics service for online scam victims, investigated the rising cases and explained in a meeting that sending sophisticated emails from unknown sources is part of a phishing attack which is already a massive cause of concern for nations.

He says: "Fake email is an extremely dangerous problem as it has the potential to infect users' computers, leaving their personal information exposed to be exploited by hackers. In terms of huge organizations and the corporate world, the damage is even more destructive."

In a board meeting of account recovery specialists, chief analyst Timothy Benson working at the firm, said: sending fake emails is the most common delivery method of initiating a cyber attack.

> Fake email is an extremely dangerous problem as it has the potential to infect users' computers, leaving their personal information exposed to be exploited by hackers"
>
> *Timothy Benson*

We may have come far in terms of technological innovation, but we remain unaware of the avenues that technology has not touched. There are certain aspects of human connection that it cannot replace. And one of them is the yearning for human connection, and emails satisfy that yearning.

Why do people receive fake emails?

Twitter doesn't essentially send such emails. This is one of the tactics that scammers use to sound genuine. According to fund recovery expert Timothy Benson, using social media platforms where most of the targets are readily available may be exploited to find potential email addresses.

They can use the information derived from Twitter and share malicious links. Twitter only sends emails from @twitter.com or @e.twitter.com. But, scammers may manipulate the icons to look similar and send fake emails with suspicious links and attachments that take the users to spam or phishing websites.

Twitter suggests that they never send emails with attachments or ask for passwords by email.

What to do if someone receives fake emails?

Here are expert recommended tips to use when someone receives a fake email.

 Do not open the email: Usually, the email header is enough to inform whether the message is from anyone known or unknown. In some cases, email receivers might be tempted to open the email, which may compromise the security of PII (Personally Identifiable Information).

 Delete the message immediately: In some cases, the malicious links infect the device's software when they are not deleted from the system. To prevent accidental message opening or malware infection, delete the email immediately.

 Never download unsolicited attachments: Email attachments accompanying the message may contain virus embedded links or spyware.

 Never click links from unknown senders: Links embedded within emails may direct email receivers to fraudulent websites. To prevent malware infection, avoid clicking any links from unknown sources.

 Do not reply to email sender: The best approach is to ignore any request from senders asking for contact numbers or provided in the message.

 Report the matter to Twitter: Users can help others by reporting the issue and bringing them to focus. Users may also check if the attempt has activity been reported by someone. Sometimes scam victims post their experiences on social media platforms to beware others.

What to do if someone clicks the links in fake emails?

Malicious links may infiltrate the users' email inboxes and steal personal details, bank details, and other financial data. Scammers can then encrypt the data and ruin the devices. Peter Thompson, who works at Cyber-Forensics.net, suggests what to do if the user has clicked on a fake email with an infected link:

 Disconnect devices from the internet: This will prevent malware from spreading to other connected devices to the network. A wireless connection can be unplugged from the main switch.

 Back up the device: When malware is suspected, erase data as quickly as possible. Get a backup and use an external device such as a USB to access files that don’t need an internet connection.

 Scan the device for additional malware: Clear the existing files and run a format. Install anti-malware software and run a scan once more. Malware is sent through legitimate look-a-like files, which can be missed easily. Therefore, pay close attention.

 Enable web-content filtering: Enable security features to protect from opening malicious links next time.

 Hire cyber experts to secure financial data: If the victims are unable to secure their financial data, they can reach out to fund recovery companies that can enable security protocol. These experts can also train victims about how to protect against such scams in future. They usually have all the information required to avoid ransomware, vishing attacks, social engineering attacks, etc.

We have heard good things about Cyber-Forensics.net in the field.

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit https://cyber-forensics.net/.

Peter Thompson

Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter
