TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

Twitter hack: Everything you need to know about this massive cyberattack

Some of the world's most influential people, including celebrities, tech pioneers, and politicians, were victims of a massive Twitter account hack on Wednesday. A few of the world's richest people, including Jeff Bezos, Warren Buffet, Bill Gates, and Elon Musk, were also victims. The accounts of politicians Joe Biden, former U.S. President Barak Obama, and celebrities such as Kanye West and Kim Kardashian West were also hacked. Many global companies such as Apple, Uber, and Tesla were also compromised by the Twitter hack.

Hackers posted similar tweets from these verified accounts requesting donations in cryptocurrencies and claimed they would give back double the amount they received from users. Potentially thousands of users were scammed after they sent money to the bitcoin wallet mentioned in the tweets.

Some of the tweets included:

"Everyone is asking me to give back," a tweet from Bill Gates' account said. "You send $1,000, I send you back $2,000."

"I am giving back to the community," was the tweet from Joe Biden and Barack Obama asking their followers to send $1,000 in bitcoins to receive $2,000.

July 2020

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

According to Twitter's internal systems, these false tweets reached over 350 million people in a few minutes. And thousands of people sent money to the hacker's bitcoin wallet.

How did this massive Twitter hack happen?

Twitter has revealed some information about the unprecedented attack that resulted in numerous hacks of high-profile verified users. Twitter's support channel in a series of tweets revealed that its internal systems were compromised.

One of the first tweets from Twitter in response to the hack said, "We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools."

What did Twitter do once the attack began?

About an hour after the attack began, Twitter took actions to lock down the affected accounts and deleted all the tweets posted by the attackers. Concerning the situation, Twitter said, "We have locked accounts that were compromised and will restore access to the original account owner only when we are certain we can do so securely."

As a safety measure, Twitter also blocked all its users from being able to tweet bitcoin wallet addresses on the platform for the time being. The company also limited the features of all the verified accounts on the platform as a precautionary measure. Twitter is currently investigating the cause of the hack and is reaching out to users in tweets on its Twitter support page.

The incident also caught the attention of the FBI, and San Francisco's FBI field office said in a statement, "We are aware of today's security incident involving several Twitter accounts belonging to high profile individuals. The accounts appear to have been compromised in order to perpetuate cryptocurrency fraud. We advise the public not to fall victim to this scam by sending cryptocurrency or money in relation to this incident."

Twitter hack: This isn't the first time

This is not the first time the social media platform has fallen prey to hackers. Twitter has been in the news several times over the past few years for being compromised by cyberattacks. Last year, Twitter chief executive Jack Dorsey's account was hacked. The company then said that it fixed the security flaw that caused the attack.

Author: Sukesh Mudrakola for Techgenix

MICROSOFT TEAMS ROLLS OUT NEW VIDEO MEETINGS FEATURES

Microsoft is rolling out a bunch of new features and options for its Microsoft Teams workplace collaboration app to reflect the new normal of remote work as well as the increase in "hybrid work," where people work from home and also spend some time at an on-premises workplace.

Many of the features are focused on video meetings in an attempt to make them more productive and less fatiguing. There are also features to boost virtual collaboration, both in groups and for accomplishing one -on-one tasks with a teammate.

Client Spotlight

easterseals
all abilities. limitless possibilities.

For 100 years, Easterseals has served as an indispensable resource for individuals with disabilities, veterans, seniors and their families.

Together, our 69 affiliates in communities nationwide serve 1.5M people through high-quality programs including autism services, early intervention, workforce development, adult day care and more.

Microsoft is rolling out a bunch of new features and options for its Microsoft Teams workplace collaboration app to reflect the new normal of remote work as well as the increase in "hybrid work," where people work from home and also spend some time at an on-premises workplace.

Many of the features are focused on video meetings in an attempt to make them more productive and less fatiguing. There are also features to boost virtual collaboration, both in groups and for accomplishing one-on-one tasks with a teammate.

Together mode

Perhaps the most intriguing of the new Microsoft Teams features is together mode, where meeting participants are digitally placed in a shared background. Microsoft says the goal is to make participants feel as if they are all sitting in the same meeting room or classroom.

"Together mode makes meetings more engaging by helping you focus on other people's faces and body language and making it easier to pick up on the non-verbal cues that are so important to human interaction," says Jared Spataro, corporate vice president for Microsoft 365.

Spataro says together mode is especially powerful for open-ended meetings, roundtables, or brainstorming discussions where all attendees speak and share viewpoints "because it makes it easier for participants to understand who is talking."

In a nod to the recent success enjoyed by Zoom as more people work from home, Microsoft is also rolling out dynamic view, aimed at the more traditional video conferences that have become ubiquitous during the COVID-19 pandemic. Dynamic view adds a slew of enhancements to the daily video meeting that gives users more options on how they share content with other participants and lets them customize the view to fit their needs. For example, Spataro says users can "show shared content and specific participants side-by-side."

Other new Microsoft Teams features

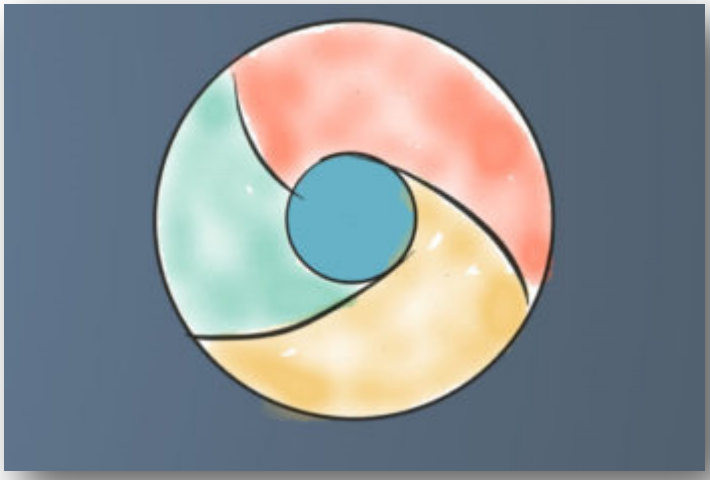
In addition to together mode and dynamic view, Microsoft is rolling out these new features for Microsoft Teams.

Video filters: Don't look your best for those early-morning or late-night meetings? With these new filters, you can adjust the lighting or soften the focus.

Live reactions: Worried your non-verbal reactions will be lost or misconstrued at large meetings? With live reactions, you can display an emoji to share your sentiment without speaking up and interrupting the meeting. Speaker attribution: An extension to the already available live captions feature, speaker attribution will let everyone know at a glance who is talking.

Speaker attribution: An extension to the already available live captions feature, speaker attribution will let everyone know at a glance who is talking.

Microsoft says these new features for Teams will begin rolling out next month. *Author: Peter King*



GOOGLE CHROME BROWSER EXTENSIONS TARGETED BY MASSIVE SPYING CAMPAIGN

Researchers from the Awake Security Threat Research Team have uncovered a massive spying campaign using malicious Chrome browser extensions. According to a post on Awake's official website, domain registrar CommuniGal Communication Ltd. (GalComm) is using Google Chrome browser extensions to surveil civilians and various industries worldwide. GalComm had been considered to be a trustworthy source, and it was this trust that was allegedly leveraged to enable the campaign, according to Awake.

Awake researchers published the following statistics about the campaign (the words in emphasis are Awake's own):

"Of the 26,079 reachable domains registered through GalComm, 15,160 domains, or almost 60%, are malicious or suspicious: hosting a variety of traditional malware and browser-based surveillance tools... In the past three months alone, we have harvested 111 malicious or fake Chrome extensions using GalComm domains for attacker command and control infrastructure and/or as loader pages for the extensions. These extensions can take screenshots, read the clipboard, harvest credential tokens stored in cookies or parameters, grab user keystrokes (like passwords), etc."

Because GalComm was considered a trusted domain registrar, anti-malware scanners did not flag the Chrome extensions as malicious. This would allow GalComm to have unmitigated access to those that downloaded its extensions. The extensions have been downloaded 32,962,951 times, and this number only includes Chrome extensions. Google has since purged the Chrome extensions from its store, but third-party extensions are still out in the wild. Google has had problems with malicious extensions in the past.

GalComm owner Moshe Fogel denied Awake's allegations in an email exchange with Reuters. In this exchange, Fogel was quoted as follows by Reuters:

> *"GalComm is not involved, and not in complicity with any malicious activity whatsoever... You can say exactly the opposite, we cooperate with law enforcement and security bodies to prevent as much as we can."*

Industries targeted by this Chrome browser extensions spying campaign, according to Awake, include "financial services, oil and gas, media and entertainment, health care and pharmaceuticals, retail, high-tech, higher education, and government organizations." This entire ordeal has called into question the vetting process that domain registrars undergo. If GalComm had been correctly flagged, none of this damage would have taken place. Security professionals are using Awake's research to determine a plan of attack that prevents something like this in the future.

Author: Derek Kortepeter