Phishing and social engineering attacks

Teenager twitter hack

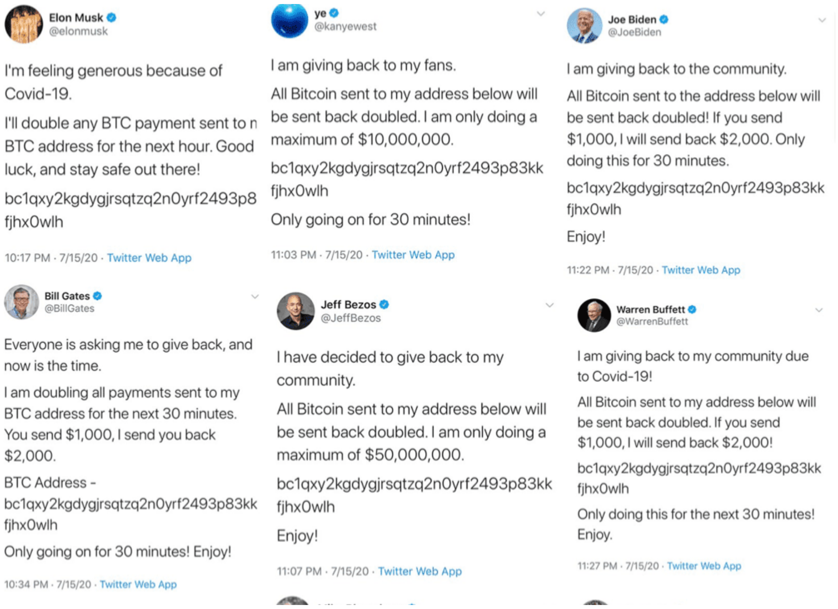
In July 2020, Twitter experienced a significant cybersecurity breach when a group of teen hackers exploited social engineering tactics to access internal tools and hijack high-profile accounts.

What Happened?

The attackers used phone spear phishing to deceive Twitter employees into revealing their login credentials. Once inside, they gained access to administrative tools that allowed them to reset passwords, bypass two-factor authentication, and take control of verified accounts.

Who Was Affected?

The breach compromised at least 130 accounts, including those of Elon Musk, Barack Obama, Joe Biden, Bill Gates, Apple, Uber, and Kanye West. The attackers used these accounts to promote a Bitcoin scam, claiming to double any funds sent to a specified address. Over $100,000 in Bitcoin was transferred before the scam was halted.



Elon Musk
@elonmusk

I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to n BTC address for the next hour. Good luck, and stay safe out there!

bc1qxy2kgdygjrsqtzq2n0yrf2493p8
fjhx0wlh

10:17 PM · 7/15/20 · Twitter Web App

ye
@kanyewest

I am giving back to my fans.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $10,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Only going on for 30 minutes!

11:03 PM · 7/15/20 · Twitter Web App

Joe Biden
@JoeBiden

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Enjoy!

11:22 PM · 7/15/20 · Twitter Web App

Bill Gates
@BillGates

Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

BTC Address -
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Only going on for 30 minutes! Enjoy!

10:34 PM · 7/15/20 · Twitter Web App

Jeff Bezos
@JeffBezos

I have decided to give back to my community.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $50,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Enjoy!

11:07 PM · 7/15/20 · Twitter Web App

Warren Buffett
@WarrenBuffett

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kk
fjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

11:27 PM · 7/15/20 · Twitter Web App

Man in the middle

Lenovo Superfish Scandal (2015):

In 2015, Lenovo, a major computer manufacturer, was caught shipping laptops with pre-installed adware called **Superfish**. This software acted as a **Man-in-the-Middle (MITM)** by intercepting secure HTTPS connections. It did this by installing its own self-signed root certificate, allowing it to decrypt and re-encrypt traffic between the user and secure websites.

This made users vulnerable because attackers on the same network could exploit this certificate to impersonate websites and **steal sensitive data like passwords and banking information**. Essentially, Superfish created a backdoor for MITM attacks by breaking the trust in HTTPS encryption.

The scandal led to lawsuits, public outrage, and forced Lenovo to release a removal tool and stop the practice. It served as a major warning about the dangers of tampering with encrypted connections and the importance of protecting against MITM threats.