PHISHING CASE STUDY

In July 2020, hackers disclosed the confidential data of 130 high-profile Twitter accounts, including Obama and Elon Musk, to run a Bitcoin scam targeting millions of followers. Twitter experienced a significant security breach due to this incident.

To execute the scheme, the attackers masqueraded as IT personnel and created a hoax internal VPN which mimicked Twitter's legitimate system. As employees logged in to the corrupted platform, the attackers were given access to Twitter's real systems, bypassing the two-factor authentication by obtaining authentication codes from the victims. This allowed the hackers to post malicious tweets encouraging a Bitcoin scam, which made approximately $110,000 in just a few hours. After this incident, 3 individuals were arrested and charged with multiple offences, including wire fraud and identity theft. This scam highlights the significant vulnerabilities in Twitter's security protocols and reinforced the importance of safeguarding and gatekeeping sensitive information.