valencia

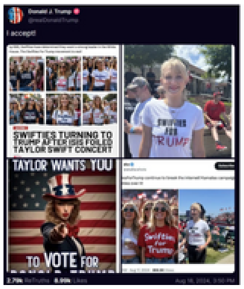
August 29, 2024

Look What You Made AI Do

Taylor Swift, Deepfakes, and Cyber Safety

Did you know that Taylor Swift weighed in on the presidential election south of the border? She didn't really, but an AI-generated image posted on Donald Trump's Truth Social account would have you believe otherwise. After their usage in the European elections, deepfakes seem to have made their way to the race to the American presidency. The threat of deepfakes is even felt in Canada: the Canadian Center for Cybersecurity has warned about it and a quarter of all Canadians report spotting them on a weekly basis. While the risk to our elections is clear, the risk for our security online is even greater.

Next Generation Social Engineering


Donald J. Trump
@realDonaldTrump
I accept!
SWIFTIES TURNING TO TRUMP AFTER ISIS FOILED TAYLOR SWIFT CONCERT
SWIFTIES FOR TRUMP
TAYLOR WANTS YOU TO VOTE FOR
Swifties for Trump
2.79k ReTruths 8.99k Likes
Aug 18, 2024, 3:50 PM

Before it was ever used as tool for political influence, AI was used to improve the sophistication of social engineering attacks. Hackers have been riding the AI wave for the last few years and the technology truly has the potential to create an actual revolution. It is also making scams more efficient, sophisticated, and convincing.

Vishing, or voice phishing, is one of the areas where deepfakes shine and where hackers rely on deepfakes and voice impersonation technologies to bypass voice authorization mechanisms. Vishing-as-a-service is becoming an offering on hacking forums that is only increasing in popularity with time: all hackers need is for an authenticator to say their name, date of birth, or a predetermined phrase, record it, and play the recording to pass themselves off as someone else.

Deepfakes have upped the ante for social engineering. Past attacks give us an idea as to how they can be used to harm people and organizations:

- In June 2015, Thamar Eilam Gindin, an Israeli professor, was deceived by an Iranian cybercriminal posing as a BBC Persian correspondent. She was tricked into sharing her email credentials, which were then used to access her social media and spread malware.
- In July 2019, cybercriminals used voice cloning to impersonate the CEO of a UK energy company and successfully tricked the company into transferring $243,000.
- The Molerats group, linked to Hamas, targeted Israeli soldiers on social media with fake personas and voice-altering software. This led the soldiers to download malware, giving attackers control over their devices.

Simply put, there are many ways that deepfakes can be used to compromise our cybersecurity. AI technologies are here to stay, though, and we must adapt to their complexities as time goes on.

Skepticism as a Swift Defence

Although the tools being used in AI-based social engineering seem impressive and are complex, we can refer to simple and basic cyber hygiene methods to remain safe.

- Limit What You Share. Strengthen your online privacy settings to limit the amount of personal data available that could be used to create convincing deepfakes. Limit the amount of personal data you share online, particularly photos and videos, as these can be used to create realistic deepfakes.
- Be Skeptical: Verify before trusting. Be skeptical of video or audio content, especially if it seems out of character for the person or is being used to make unusual requests. Look for inconsistencies or signs of manipulation. Before sharing any personal or financial information, verify the request's authenticity through a trusted method. For example, if a caller claims to be from your bank, hang up and call the bank back using their official phone number.
- Stay aware and apply hygiene. Stay informed about the latest social engineering tactics and educate those around you. Avoid engaging with unsolicited messages or calls, particularly those that try to create a sense of urgency to pressure you into makg quick decisions.
- At work, are there policies and training in place? If staff know that you will never make unusual requests over email because it's against policy, you reduce risk.

As AI continues to advance, our commitment to cyber safety must evolve in tandem by staying informed, adopting skeptical practices, and informing others.