imagine IT

The Q2 2024 State of Cybersecurity

imagineiti.com

Deepfakes Are Getting Real

Earlier this year, social engineering followed by a deepfake video conference call led to the loss of over $25,000,000 from a large firm. Incidents of smaller scale are now victimizing small and medium size businesses.

What is a Deepfake?

A Deepfake is a type of synthetic media in which a person in an audio, image, or video is replaced with someone else's likeness using artificial intelligence (AI), thereby potentially fooling the listener/viewer into believing the live person is someone else. There are now many easy to obtain software applications that can quickly generate Deepfake content and manipulate live conversations.

Why Should We Be Concerned with Deepfakes?

Deepfakes can cause political manipulation, reputation damage, and harassment. But for the purposes of this article, I will focus on financial fraud. Here are some of the primary methods:

Impersonation in Video or Audio Calls:

Executive Fraud: Fraudsters can use deepfakes to impersonate high-ranking executives during video conferences or phone calls. They may instruct employees to transfer funds to fraudulent accounts, believing they are following legitimate orders from their boss.

Client or Vendor Scams: Scammers can impersonate clients or vendors in video calls to redirect payments or change bank account details, convincing the target to send money to a fraudulent account.

Synthetic Identity Fraud

Deepfakes can create entirely synthetic identities by blending features of multiple real people. These fake identities can be used to open bank accounts, apply for loans, or create fraudulent credit card accounts, which are then used to steal money or launder funds.

Manipulating Verification Processes:

Know Your Customer (KYC) Evasion: Financial institutions often use video calls for KYC processes to verify the identities of their customers. Deepfakes can fool these systems by presenting a realistic but fake identity, allowing fraudsters to pass these checks and gain access to financial services under false pretenses.

Biometric Spoofing: Some institutions use biometric data, like facial recognition, for security. Deepfakes can be used to create fake biometric data that passes these systems, allowing unauthorized access to accounts.

Phishing and Social Engineering:

Enhanced Phishing Attacks: Deepfakes can be used to create highly convincing phishing messages. For example, a deepfake video of a CEO might be sent to employees instructing them to click on a malicious link or provide sensitive information.

Confidence Scams: Fraudsters can use deepfake videos or audio to gain the trust of victims by pretending to be a trusted individual. Once trust is established, they can manipulate the victim into transferring money or sharing financial information.

How Do We Avoid Becoming a Deepfake Victim?

To mitigate these risks, organizations need to employ robust verification processes including multi-factor authentication (MFA), in-person verification, and eliminating facial recognition as a form of MFA. Additionally, training employees to recognize and respond to potential deepfake scams is crucial for maintaining security.

Impersonation Finance Fraud

What is Impersonation Finance Fraud?

Impersonation financial fraud involves someone pretending to be another person to gain access to their financial resources or sensitive information for illicit gain. This type of fraud can take various forms and typically involves the perpetrator assuming the identity of an individual or a representative of a legitimate entity. Here are some common types of impersonation financial fraud:

Phishing and Vishing:

Phishing: Fraudsters send messages pretending to be from legitimate financial institutions, asking the recipient to provide personal information, such as login credentials or credit card numbers.

Vishing: Similar to phishing but conducted over the phone, the scammer might impersonate a bank representative, asking for account details or other sensitive information.

Romance Scams:

Scammers create fake online profiles on dating sites and social media to build romantic relationships with victims, eventually convincing them to send money or disclose financial details.

Business Email Compromise (BEC):

Fraudsters hack into or spoof email accounts of company executives or trusted partners and send fraudulent emails to employees, customers, or vendors, instructing them to transfer funds, change banking information, or disclose sensitive financial information.

Tech Support Scams:

Fraudsters impersonate tech support representatives from well-known companies or from IT Support, claiming there is a problem with the victim's computer or account and requesting payment for unnecessary or nonexistent services.

Impersonating Government Officials:

Scammers pretend to be from government agencies (e.g., IRS, Social Security Administration) and threaten victims with fines, arrest, or other penalties unless they make immediate payments or provide personal information.

Fake Debt Collectors:

Fraudsters pose as debt collectors, demanding payment for fake or inflated debts. They often use threats and high-pressure tactics to coerce victims into paying.

Synthetic Identity Theft:

A type of identity theft where criminals combine real and fake information to create a new identity. For instance, they might use a real Social Security number but a fake name and address to apply for loans or credit cards.

CEO/Executive Fraud:

A specific form of BEC where fraudsters impersonate a CEO or high-ranking executive, instructing employees to make urgent wire transfers or reveal confidential information under the guise of a critical business need.

How Do We Avoid Becoming an Impersonation Finance Fraud Victim?

Preventing impersonation financial fraud involves being cautious about sharing personal information, verifying the identity of individuals or entities before engaging in financial transactions, using strong and unique passwords, and being aware of common fraud tactics. Regular monitoring of financial accounts and credit reports can also help detect and address fraud early.

Some Tactical Recommendations:

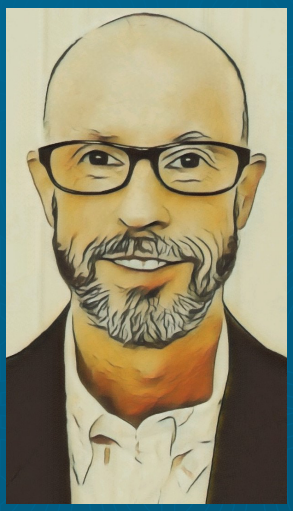
- If the requester claims to be someone you trust, verify the request by CALLING BACK TO A PHONE NUMBER ALREADY IN YOUR POSSESSION or visit them in-person.
- Freeze your credit at the 3 credit bureaus.
- Perform frequent user cybersecurity training (see next topic).

Group Cybersecurity Training Sessions

Many organizations provide their employees recurring Phishing Campaigns and Training Videos w/Quizzes. This is an effective way to keep cyber cautiousness front of mind. However, it is important to provide an engaged instructor led session, 1-2 times per year, to fill gaps and provide content for new threats.

What Are Some Good Topics to Include in a Training Session?

- Multi-Factor Authentication (MFA)
- Password Bad Habits & Bests Practices
- Online Ads
- Investment Scams
- Email Best Practices
- Inbound Calls Best Practices
- Cell Phone Best Practices
- QR Codes
- Deepfakes
- Chat Tool Phishing
- Remote Work Threats
- Home Office & Guest WiFi
- User Mistake Stories



Peter's Insight

Cyber protection technologies only go so far. Most incidents originate from a user mistake and can be extremely costly. In the U.S. in 2023, fraud incidents accounted for 20 times more financial loss compared to Ransomware. Therefore, a multifaceted approach to security awareness is critical.

I personally perform dozens of group cybersecurity training webinars each year to businesses and associations (which includes some end-user homework), and the feedback has always been extremely positive. Please reach out to me if you are interested in a "subject matter expert" led training session.

Conclusion

Deepfakes and finance fraud poses significant risks to individuals and businesses. Key pitfalls include substantial financial losses, damage to credit ratings, and the lengthy, complex process of restoring compromised accounts. To avoid falling victim to such fraud, it's crucial to implement strong, multi-layered security measures. These include using strong, unique passwords for all financial accounts, enabling multi-factor authentication (MFA), and monitoring account activity for suspicious transactions. Additionally, individuals and organizations should be wary of phishing attempts and ensure sensitive information is shared only through secure, verified channels. Employing robust identity verification processes and educating users and stakeholders about common fraud tactics can further bolster defenses against deepfakes and finance fraud.