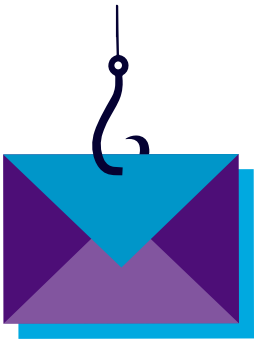
SUPERCHARGING SCAMS: HOW CRIMINALS USE MODERN TECHNOLOGY TO DECEIVE AND MANIPULATE THEIR VICTIMS

Technology plays a huge role in how scams are executed. Criminals use a variety of tools and platforms that enable scalability, automation and improved credibility – all of which helps them deceive and manipulate people, increase the complexity of their ploys and avoid detection. Recognizing how technology can help enable scams is critical to preventing them.

DIGITAL COMMUNICATIONS CAN CREATE ADDITIONAL PLATFORMS FOR IMPOSTOR SCAMS



- **Phishing** (emails) and **smishing** (texts) are fake messages that appear to come from trusted entities, such as financial institutions, delivery services or government. These messages prompt the recipient for personal or financial information and are relatively low cost for the criminals to initiate.
- **Auto-dialers** and **caller ID spoofing** are used by criminals to disguise their identities and "robocall" a large volume of people at once. Caller ID spoofing occurs when the criminal changes the number on the caller ID that is displayed during a phone call to make it appear to be from a trusted number. These tools can make it appear the call is coming from a legitimate business, government agency, family member or friend.
- **Social media manipulation** occurs when criminals create fake profiles or bots (automated software applications) to gain trust, gather information and carry out scams. Criminals may use these tools to impersonate friends, celebrities or public officials to trick people into sending money or providing personal or financial information.

MALWARE AND OTHER TACTICS PROVIDE ACCESS TO ACCOUNTS, DEVICES AND SENSITIVE DATA

- **Malware** (malicious software) and **spyware** can be installed by criminals when victims download manipulated software applications or click on malicious email links or attachments. These tools can steal passwords, bank information and other data that can be used to take over an account and send unauthorized payments, open fraudulent accounts or create synthetic identities.
- **Remote access trojans** (RATS) are malware that criminals use to take control of a victim's device -- and often are used in tech support scams.
- **SIM (subscriber identity module) card swapping**, **porting** and **call forwarding** are all legitimate services, but criminals may use them to take over a mobile phone and control accounts belonging to the victim. Financial institutions and other entities often use one-time passcodes to authenticate the user. If the criminal has access to the phone, he is able to intercept the passcode, pose as the victim and initiate fraudulent transactions.

SUPERCHARGING SCAMS: HOW CRIMINALS USE MODERN TECHNOLOGY TO DECEIVE AND MANIPULATE THEIR VICTIMS

FAKE WEBSITES, ONLINE PLATFORMS AND APPS HELP BRING CREDIBILITY TO SCAMS

- **Screen-scraped or copied websites** are identical replicas of real sites that criminals use to collect login credentials or payments. Smishing text messages or phishing emails provide a link that takes the user to a fake site that prompts for online banking credentials typically use screen-scraping or copied images to appear identical to the legitimate site.
- **Online marketplaces and ads**, although often legitimate, also can provide a platform for criminals to post listings for jobs, products or rentals that don't exist.
- **Investment platforms** may actually be sophisticated scam sites, applications or fake digital wallets that are created to build long-term deceptions and steal money over time by making the victims believe they are earning money on funds they have invested.
- **Fraudulent mobile apps and quick response (QR) codes** may use a legitimate name or brand to steal personal information, intercept payments or install malware that gives criminals control of internet-connected devices and gadgets.

GENERATIVE ARTIFICIAL INTELLIGENCE (AI) FURTHERS SOCIAL ENGINEERING TECHNIQUES

- **Voice cloning** is an AI-generated voice that mimics a person's real voice. This can be used to impersonate family, friends or executives in "emergency"-based scams.
- **Deepfake videos or images** use generative AI to generate a likeness of a real person. These can be used to impersonate a public figure to promote a fake investment scheme, a family or friend to manipulate trust, or a customer to authenticate and gain access to financial accounts. These digitally created images and videos are sophisticated and often appear to be real people because of their realistic characteristics – such as hand gestures and unique speech patterns.

Explore more about how criminals are using generative AI to increase the scale of their attacks by automating the creation and execution of fraud through synthetic identities:

When Synthetic Identities and Artificial Intelligence Collide | FedPayments Improvement

Generative Artificial Intelligence Increases Synthetic Identity Fraud Threats

- **Generative AI communication** can be used to launch large-scale attacks, contacting people and businesses through social media, phone, text messages and email. Generative AI also can be programmed to manage these communications to convince people to send money based on investment opportunities, romantic interests or other scams; share personal information or account login details; or download malware to their computers or devices.

CRYPTO, VPNS AND BOTNETS PROVIDE ANONYMITY AND SCALE

- **Cryptocurrency, digital wallets and money transfer applications** often are used by criminals to make it more difficult to trace funds.
- **Virtual private networks (VPNs) and botnets** help hide criminals' true locations and enable them to automate attacks to target a large volume of people at the same time.
- **Dark web sites, chatrooms and marketplaces** are used to share successful tactics, develop criminal networks and sell stolen data, malware and services.
- **Credential stuffing** is an automated cyberattack that typically uses bots or botnets to rapidly test stolen login credentials across multiple websites or apps, including online banking for accounts at financial institutions.

CONCLUSION

Criminals will continue to exploit emerging technology, vulnerabilities and social engineering to manipulate and deceive their victims. These tools – many of which were designed to enhance our everyday lives – can be turned into powerful mechanisms that make scams more convincing, scalable and difficult to trace. Staying informed about these capabilities is a vital component to build defenses that can reduce the impact of these threats and the scams they enable.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.