State of Online Scams 2024

Table of Contents

Record $12.5 Billion Stolen from Americans

Americans lost a record $12.5 billion to online scams in 2023, an increase from $10.3 billion in 2022, according to the Federal Bureau of Investigation Internet Crime Complaint Center (IC3).

Despite increased national awareness and regular warnings from the government, financial institutions and private companies in the Internet safety space, the perpetrators have been able to keep flourishing, setting new records year after year.

In recent years, investment scams have skyrocketed to No. 1 with Americans losing a record $4.57 billion in 2023, up from $3.3 billion. An unprecedented 86.7% of investment scams involved crypto which may be why Millennials fell for more investment scams than any other generation last year.

Despite their tech prowess, the number of teen and Gen-Z online scam victims also surged by nearly 10% last year, which shows that scammers have grown increasingly sophisticated, and this can also be tied to a rise in sextortion scams, which has led many teens to commit suicide.

This national crisis is likely to get worse in the years ahead as scammers can now use artificial intelligence to create deepfake videos of business leaders, celebrities, politicians and romantic suitors that are difficult to detect. Legendary investor Warren Buffett said recently that AI’s use in scams is going to be the biggest “growth industry of all time.”

Online scams are a global crisis but America is by far the most targeted nation due to its affluence and reliance on technology. According to the FBI Internet Crime Report from 2023, Americans filed 521,652 complaints, while the next 19 most impacted nations filed 315,335 complaints combined.

Online scams impact certain states more than others. California is the No. 1 most-scammed state with victims losing $2.2 billion last year, followed by Texas, Florida and New York.

Our analysis of the most recent FBI data revealed that more that 95.7% of money lost in 2023 was never recovered. This is due to most scammers living overseas, where U.S. law enforcement has no jurisdiction, and it speaks to a lack of international government cooperation.

With too many Americans losing their life savings, and law enforcement unable to recover the stolen funds in most cases, it is critical that people take this seriously and learn to spot and avoid scams before they occur.

Social Catfish – a company dedicated to eradicating online scams using reverse search technology – is releasing this study after analyzing the most recent data from the FBI Internet Crime Complaint Center (IC3) and the Federal Trade Commission (FTC) through 2023 and after conducting a proprietary poll of (X amount) romance scam victims in August 2024.

Key Findings:

- **5 Costliest Online Scams:** Investment ($4.57 billion), BEC scams ($2.95 billion), Confidence Fraud/Romance ($653 million), Tech Support ($925 million), and personal data breach ($744 million)
- **5 Most-Scammed States:** California ($2.1B), Texas ($1 billion), Florida ($875 million), New York ($750 million), and New Jersey ($441 million).
- **5 Most-Scammed Countries:** US (521,652 victims), UK (288,355), Canada (6,601), India (3,405), and Nigeria (1,779).
- **Crypto Accounted for 86.7% of Investment Scams:** A record $3.96 billion was lost last year to fake crypto investment scams.
- **Surge in Tech-Savvy Teen, Gen-Z and Millennial Victims: Millennials fell for more investment scams than any generation**: Victims ages 30-49 filing more than 13,000 complaints last year. The number of teen and Gen-Z victims across all online scams surged by nearly 10% last year to 80,584 alongside a rise in sextortion scams.
- **95.7% of Stolen Funds Were Not Recovered in 2023:** The FBI IC3 Recovery Asset Team was able to recover $538.39 million, or 4.3%, of the total $12.5 billion lost by victims in 2023. This is because most scammers reside internationally and there is a lack of cooperation between countries to bring scammers to justice.

Which States Lost the Most Money to Online Scams?

California was the hardest hit state with more than 75,000 victims losing a staggering $2.2 billion last year. The rest of the top five included other large states including Texas, Florida, New York and New Jersey.

On the other end of the spectrum, North Dakota lost the least amount of money and had just over 700 victims. Still, residents in the state lost a heft $14.3 million which shows that even smaller states are experiencing large losses. Vermont, Alaska, Wyoming and West Virginia round out the five states that were the least amount of money lost.

States With The Most Victims Per Capita

When it comes to which states are most susceptible to online scams, we take into account the number of reports filed with FTC and population size to present an accurate measure. 6 of the top 10 states are on the east coast and the top two states are neighbors in the southeast.

Based on complaints filed with the FTC in 2023, Georgia ranks No. 1 in the nation filing 1,564 reports per 100,000 residents. Their neighbor also in the south east is Florida which ranks No. 2. On the other end of the spectrum, five of the 10 states with the fewest reports per capita are in the midwest, including the top three spots taken by South Dakota, North Dakota and Iowa. Kansas filed the 5th fewest reports and Nebraska came in at No. 7.

100 Metropolitan Areas with the Highest Rates of Online Scam Complaints

Analysis of the data found that certain cities and metropolitan areas are hotbeds for online scams. Among the top 100, Florida has 21 metropolitan areas on the list, this represents more than 20% of the list. Georgia, North Carolina and South Carolina all had seven metropolitan areas represented, California had six, while Texas, Arizona, Alabama, and Louisiana had five.

Top 10 Most Financially Devastating Online Scams

Investment fraud has skyrocketed in recent years and is the No. 1 costliest type of fraud in America for the second year in a row, according to the FBI. A record $4.57 billion was lost to investment fraud in 2023, up from $3.3 billion in 2022 and a staggering 18 times higher than $253 million in 2018.

Business Email Compromise (BEC), which previously held the top spot as of 2021, ranks No. 2 ($2.95 billion) confidence fraud/romance scams ranks No. 3 ($652.5 million), tech support ranks No. 4 ($924.5 million) and personal data breach rounds out the top five ($744.2 million).

1. Investment Scams

How They Work: Fraudsters contact victims via social media, business networking sites, dating apps, and via email and text promising “can’t miss” investment opportunities with enormous returns and little or no risk. Scammers then disappear with the money, or send fake reports to get people to keep investing.

5 Types of Investment Scams:

- Ponzi schemes promise high returns with little risk by paying earlier investors with the funds from newer investors, rather than from actual profit earned. These schemes eventually collapse when there aren't enough new investors to pay returns to earlier ones. To avoid falling victim, be skeptical of investments that guarantee high returns with no risk.

- Pyramid schemes involve recruiting participants who are promised payments for enrolling others into the scheme rather than selling a legitimate product or service. These scams rely on a constant influx of new participants to fund payouts, and they collapse once recruitment slows down. It’s important to be cautious of any investment opportunity that emphasizes recruitment over a tangible product or service.

- In pump and dump schemes, fraudsters artificially inflate the price of a low-value stock through false and misleading statements, only to sell their shares at the peak price, leaving other investors with worthless stocks. These schemes are often promoted through social media and online forums. Always conduct thorough research before investing in low-value stocks being hyped online.

- Advance-fee fraud involves scammers who promise victims a significant return on investment, but only after they pay an upfront fee. Once the fee is paid, the scammer disappears without providing the promised return. To protect yourself, never pay upfront fees for the promise of future returns.

- Offshore investment scams lure victims with promises of tax-free returns from investments located in foreign countries. These investments are often fraudulent, and victims find it difficult to recover their money due to international legal barriers. Before investing in any offshore opportunities, seek advice from a trusted financial professional and verify the legitimacy of the investment.

Tips to Avoid Them: Consult a third-party financial professional before investing; do research and verify the company and person you are investing with; if something seems too good to be true, it usually is.

2. Business Email Compromise Scams (BEC)

How They Work: Fraudsters pose as company executives or trusted business partners and send fraudulent emails to employees, instructing them to transfer funds to accounts controlled by the scammers. These emails often appear legitimate and urgent, leveraging authority and trust to bypass normal verification procedures.

5 Types of BEC Scams:

- In CEO fraud, scammers impersonate a company's CEO or high-ranking executive and send an urgent email to an employee, typically in finance or HR, instructing them to wire money to a specific account. The email often stresses confidentiality and urgency to prevent the employee from questioning the request. It's crucial to implement strict protocols for verifying such requests, including direct verbal confirmation.

- In an account compromise scam, a cybercriminal gains access to an employee's email account and uses it to send fraudulent invoices or requests for payment to vendors or clients. The recipients, believing the request to be legitimate, transfer funds to accounts controlled by the scammers. Regular monitoring and multi-factor authentication can help prevent unauthorized access to email accounts.

- Invoice fraud occurs when scammers impersonate a supplier or vendor and send a fake invoice to a company's accounts payable department. The invoice appears to be for legitimate goods or services, but payment is directed to a bank account controlled by the fraudsters. Companies should verify all invoice details, especially changes to payment accounts, by contacting the vendor directly through a verified method.

- In data theft BEC scams, attackers target HR or finance employees, requesting sensitive information such as employee tax records, payroll details, or personally identifiable information (PII). This information can then be used for identity theft, tax fraud, or further spear-phishing attacks. Limiting access to sensitive data and implementing strict verification procedures for data requests can help protect against this type of scam.

- In lawyer impersonation scams, fraudsters pose as legal representatives or external law firms handling confidential or sensitive matters. They contact employees, often in the finance department, and instruct them to make urgent, confidential payments, often under the guise of settling a legal matter. Educating employees about this tactic and verifying requests through independent channels can prevent such scams from succeeding.

Tips to Avoid Them: Implement a multi-step verification process for fund transfers, educate employees on how to recognize phishing emails, and encourage verification of transfer requests through a secondary communication method, such as a phone call to the requester.

3. Tech Support Scams

How They Work: Scammers pose as tech support agents from reputable companies, claiming that your computer has a virus or other issues. They convince victims to grant remote access to their computers and charge for unnecessary repairs or install malware to steal personal information.

5 Types of Tech Support Scams:

- Scammers create fake pop-up warnings that appear on your computer, warning you that your system is infected with a virus or malware. These pop-ups often mimic legitimate security alerts and instruct you to call a toll-free number for immediate assistance. Once you call, the scammer will try to sell you unnecessary software or gain remote access to your computer to steal your personal information.

- In cold call scams, fraudsters call you directly, claiming to be from a well-known tech company like Microsoft or Apple. They tell you that they have detected problems with your computer, such as viruses or outdated software, and offer to fix the issue remotely. They often ask for payment for their "services" and may install malware or steal sensitive information once they gain access to your computer.

- Scammers send fake emails that appear to be from legitimate tech support companies, warning you of supposed issues with your computer or account. These emails often contain links that lead to phishing websites where you're prompted to enter personal information or download malicious software. Alternatively, the email may direct you to call a fake tech support number where the scammer tries to gain remote access to your device.

- Scammers set up fake websites that appear to be official tech support pages for reputable companies. These sites often rank high in search engine results for queries like "Microsoft tech support" or "Apple help." When you visit these sites and call the listed number, you're connected to a scammer who will attempt to charge you for unnecessary services or install malware on your device.

- In this type of scam, the fraudster convinces you to install remote access software, claiming it’s necessary to fix your computer. Once the software is installed, the scammer has full control of your computer and can steal your data, install malware, or lock you out of your system entirely. They may then demand payment to restore access or remove the supposed issue.

Tips to Avoid Them: Never give control of your computer to someone who contacts you unexpectedly, verify the identity of any tech support agent through official company channels, and use reputable security software to protect your devices.

4. Personal Data Breach

How They Work: Hackers steal personal information such as Social Security numbers, credit card details, and login credentials through data breaches of companies' databases. This information is then used for identity theft, financial fraud, or sold on the dark web.

5 Types of Personal Data Breach Scams

- Phishing scams involve hackers sending fraudulent emails or messages that appear to be from a trusted organization, such as a bank or social media platform. These messages often contain links to fake websites where victims are prompted to enter their personal information, such as login credentials or credit card numbers. Once the information is entered, it's captured by the scammer and used for identity theft or sold on the dark web.

- In ransomware attacks, hackers infiltrate a company's database or a user's device and encrypt their personal data, rendering it inaccessible. The attackers then demand a ransom in exchange for the decryption key. Even if the ransom is paid, there's no guarantee that the data will be restored, and the stolen information may still be sold on the dark web.

- MitM attacks occur when a hacker intercepts communication between two parties, such as a user and a website, to steal personal information. For example, if a user connects to an unsecured public Wi-Fi network, a hacker can intercept the data being transmitted, including login credentials and credit card details. This stolen information is then used for financial fraud or identity theft.

- Malware infections involve the use of malicious software to gain unauthorized access to a user's personal data. This malware can be installed on a user's device through phishing emails, malicious websites, or infected downloads. Once installed, the malware can steal sensitive information such as passwords, Social Security numbers, and bank account details, which the hacker can then exploit or sell.

- Insider threats occur when an employee or contractor within a company intentionally leaks or steals personal data. This can happen if the individual is disgruntled or is being paid by an external party to share confidential information. Insider threats are particularly dangerous because the perpetrators often have legitimate access to sensitive data, making it difficult to detect the breach until the damage is done.

Tips to Avoid Them: Use strong, unique passwords for different accounts, enable two-factor authentication, monitor your financial statements regularly for unauthorized transactions, and freeze your credit if you suspect your information has been compromised.

5. Confidence Fraud/Romance Scams

How They Work: Scammers create fake profiles on dating sites and social media to establish relationships with victims. Over time, they build trust and then fabricate emergencies, asking for financial help. Once the money is sent, the scammer often disappears. However, sometimes they stick around, making excuses to request more money while avoiding any in-person meetings.

- The scammer creates a fake online identity on dating sites or social media platforms to lure victims into emotional or romantic relationships. Once trust is established, they manipulate the victim into sending money, gifts, or personal information.

- Scammers pose as military personnel stationed overseas, often using stolen photos of real soldiers. They fabricate stories about needing money for leave, medical emergencies, or other fabricated expenses.

- Scammers target individuals who are grieving the loss of a spouse. They exploit the victim's vulnerability by pretending to be a widow or widower themselves, using sympathy to build trust and eventually ask for financial help.

- The scammer claims to be in love with the victim and tells a story about receiving a large inheritance. They then request money for legal fees or other expenses needed to access the inheritance, promising to share the wealth once it’s received.

- The scammer pretends to be a foreign love interest and claims they need financial assistance to obtain a visa or pay for travel expenses to come to the victim's country. Once the money is sent, the scammer disappears.

Tips to Avoid Them: Be cautious of anyone who quickly professes love, never send money to someone you haven't met in person, and do a reverse image search on their profile pictures to check for authenticity.

6. Data Breach

How They Work: Hackers steal personal information such as Social Security numbers, credit card details, and login credentials through data breaches of companies' databases. This information is then used for identity theft, financial fraud, or sold on the dark web.

- Scammers send fake emails or messages that appear to be from reputable companies, tricking victims into revealing personal information like passwords, credit card numbers, or Social Security numbers. This data is then used for identity theft.

- Cybercriminals breach a company’s database and encrypt sensitive data, demanding a ransom for its release. If the ransom isn’t paid, the data may be sold on the dark web or publicly released.

- Hackers use stolen login credentials from one breach to access accounts on other websites, banking on the fact that many people reuse passwords across multiple sites.

This leads to further unauthorized access and data theft.

- Hackers impersonate trusted individuals or organizations to manipulate victims into divulging confidential information. This information is then used to access accounts, steal identities, or commit financial fraud.

- Scammers gain control of a victim's phone number by convincing the phone company to switch the number to a new SIM card. This allows the scammer to bypass two-factor authentication and gain access to the victim's accounts.

Tips to Avoid Them: Use strong, unique passwords for different accounts, enable two-factor authentication, monitor your financial statements regularly for unauthorized transactions, and freeze your credit if you suspect your information has been compromised.

7. Government Impersonation Scams

How They Work: Scammers pose as government officials from agencies like the IRS, Social Security Administration, or law enforcement. They contact victims claiming they owe money, need to verify personal information, or face arrest if they don't comply. They often use threats and high-pressure tactics to instill fear.

- Scammers pose as IRS agents, claiming that the victim owes back taxes and must pay immediately to avoid arrest. They often demand payment via gift cards, wire transfers, or cryptocurrency.

- The scammer claims to be from the Social Security Administration, warning the victim that their Social Security number has been suspended due to suspicious activity. They demand personal information or payment to resolve the issue.

- Victims receive a call or message from someone claiming to be a law enforcement officer, stating that they failed to appear for jury duty and must pay a fine immediately to avoid arrest.

- Scammers pose as Medicare representatives and ask for personal information or payment, claiming that new Medicare cards are being issued or that benefits are about to be cut off.

- Scammers impersonate officials from immigration services, threatening deportation unless the victim pays a fine or provides personal information to "correct" their immigration status.

Tips to Avoid Them: Remember that government agencies will never call and ask for personal information or demand immediate payment. Verify the identity of the caller by contacting the agency directly using official contact information. Do not provide personal information or payment over the phone.

8. Non-Payment/Non-Delivery Scams

How They Work: In non-payment scams, sellers do not receive payment for goods or services sold online. In non-delivery scams, buyers pay for goods or services online but never receive them. These scams often occur on auction sites, classified ads, and social media marketplaces.

- Scammers set up fake websites that look like legitimate online stores. Victims make a purchase, but the items are never delivered, and the website disappears shortly after.
- The scammer lists high-value items on auction sites, collecting payment from the highest bidder but never delivering the goods. Often, the items are counterfeit or don't exist at all.
- Scammers post fake ads for popular items on classified sites. When the victim tries to buy the item, they're instructed to send money, often via wire transfer, but never receive the product.
- The scammer pays for a service or product, receives the item, and then reverses the payment through their bank or credit card company, leaving the seller without payment.
- The scammer sends fake invoices to businesses or individuals for products or services that were never ordered or delivered, hoping the recipient will pay the invoice without checking its legitimacy.

Tips to Avoid Them: Use secure payment methods that offer fraud protection, avoid paying with wire transfers or gift cards, and research the buyer or seller before completing a transaction. Use reputable and well-known platforms that offer buyer and seller protection.

9. Credit Card/Check Fraud

How They Work: Scammers obtain your credit card or bank account information and use it to make unauthorized purchases or withdraw money. This can happen through phishing emails, skimming devices on ATMs or point-of-sale terminals, or data breaches.

- Scammers install skimming devices on ATMs or point-of-sale terminals to steal credit card information when the card is swiped. The stolen data is then used to make fraudulent purchases.
- Scammers send emails that appear to be from legitimate companies, asking recipients to update their payment information. The information entered is then used to commit fraud.
- Scammers send victims fake checks, often as payment for goods or services. The victim deposits the check, which initially clears, but is later found to be fraudulent, leaving the victim responsible for the amount.

- Scammers use stolen credit card information to make online or over-the-phone purchases, where the physical card is not required.

- Scammers gain access to a victim's bank or credit card account by stealing login credentials. They then make unauthorized purchases or transfer funds out of the account.

Tips to Avoid Them: Regularly monitor your bank and credit card statements for unauthorized transactions, report lost or stolen cards immediately, use credit cards with chip technology, and be cautious when sharing financial information online or over the phone.

10. Real Estate Scams

How They Work: Scammers pose as landlords or real estate agents and offer properties for rent or sale that they do not own or have no authority to lease. They collect deposits and rent payments from victims and then disappear, leaving the victim without a property and out of pocket.

- Scammers post fake rental listings, often for properties they don't own. They collect deposits and rent payments from victims but never provide access to the property.

- Scammers forge documents to transfer ownership of a property without the owner's knowledge, then take out loans against the property or sell it to an unsuspecting buyer.

- Scammers prey on homeowners facing foreclosure, promising to negotiate with lenders to save their homes. They charge high fees and disappear without providing any help.

- Scammers offer fake real estate investment opportunities, promising high returns. They collect money from investors and then disappear, leaving the victims with nothing.

- Scammers pose as real estate agents, convincing victims to wire money for deposits, down payments, or closing costs. Once the money is sent, the scammer disappears, and the victim is left with no property and no money.

Tips to Avoid Them: Verify the legitimacy of the property and the landlord or agent by visiting the property in person, researching property records, and using licensed real estate professionals. Never send money without confirming the legitimacy of the transaction.

States with the Most & Least Crypto Scams Per Capita

An unprecedented 86.7% of all money lost to investment scams in 2023 involved crypto – totaling a record $3.96 billion. Chances are, if you are contacted or see an advertisement for a crypto investment, it is a scam.

Fraudsters have also become adept at using crypto in romance scams by entering fake romantic relationships with their targets, usually via online dating platforms, social media, or messaging apps, with the ultimate goal of convincing the victim to invest in fraudulent cryptocurrency schemes.

Many people have lost their life savings to crypto scams. In one case, a father from Virginia committed suicide after losing his life savings after investing in crypto as part of a romance scam.

10 Most Common Crypto Scams in 2024

Romance Scams

In romance scams, fraudsters build a fake relationship with the victim over time, often posing as attractive and sympathetic characters. These scammers use emotional manipulation to gain the trust and affection of their victims. Once trust is established, they fabricate emergencies or financial crises, convincing the victim to buy and send Bitcoin as a means of support. Victims, believing they are helping a loved one, willingly transfer Bitcoin to the scammer’s wallet, only to realize later that they have been deceived. These scams are prevalent on dating websites and social media platforms, making it difficult for victims to discern the true intentions of their online acquaintances.

Investment Scams

Investment scams lure victims with promises of high returns and lucrative opportunities. Scammers create convincing websites, testimonials, and social media profiles to present themselves as credible investment firms or financial advisors. They persuade victims to invest by purchasing Bitcoin and transferring it to the scammer’s wallet. The victims are often shown fake earnings reports to encourage further investments. Once a significant amount of Bitcoin is collected, the scammers disappear, leaving the victims with substantial financial losses. This method exploits the growing interest in cryptocurrency investments and the lack of understanding many people have about the industry. A particularly deceptive variant of investment scams is known as "pig butchering" scams. Scammers build long-term relationships with victims to gain their trust, posing as friends, romantic interests, or mentors. Over time, they introduce a fake investment opportunity, often involving cryptocurrency. As the victims grow more confident, they are encouraged to invest larger sums. Once the scammer decides they've extracted as much as possible, they disappear with all the funds, leaving victims financially and emotionally devastated. This scam is especially cruel as it exploits both the victim's money and their trust.

Blackmail and Sextortion

Blackmail and sextortion scams involve threatening victims with the release of sensitive or compromising information or photos unless they pay a ransom in Bitcoin. Scammers obtain these materials through hacking, phishing, or deceitful interactions. Once they have the incriminating data, they contact the victim, demanding payment in Bitcoin to keep the information private. The anonymity of Bitcoin transactions makes it difficult to trace the recipients, making this method attractive to scammers. This type of scam can cause significant emotional distress and financial harm to victims, who often feel they have no choice but to comply with the demands.

Fake Online Marketplaces

Scammers create fake online marketplaces that appear legitimate, offering goods or services at attractive prices. Victims are enticed to purchase items using Bitcoin, thinking they are getting a great deal. After the transaction, the scammers disappear, leaving the victims without the goods or services they paid for. These fake marketplaces can be very convincing, with professional-looking websites and fake customer reviews. The irreversible nature of Bitcoin transactions means that once the payment is made, it is nearly impossible for victims to recover their money.

Impersonation of Authorities

In these scams, fraudsters impersonate government officials, law enforcement agents, or other authorities, claiming that the victim is in legal trouble. They threaten severe consequences, such as arrest or legal action, unless the victim pays a fine or fee in Bitcoin. The urgency and fear created by these threats often compel victims to comply without verifying the legitimacy of the claims. This scam exploits the trust and fear people have towards authorities, making them more likely to follow the instructions without questioning them.

Technical Support Scams

Technical support scams involve scammers contacting victims under the guise of providing tech support. They claim that the victim’s computer or device is infected with a virus or has technical issues that need immediate attention. The scammers then instruct the victims to pay for the service or necessary software using Bitcoin. They may also gain remote access to the victim’s device to further exploit them. These scams prey on people’s lack of technical knowledge and their fear of losing important data or functionality of their devices.

Phishing Scams

Phishing scams involve sending emails or messages that appear to be from legitimate companies or services, requesting Bitcoin payment for account verification, upgrade, or to avoid account suspension. These emails often contain links to fake websites that closely mimic the real ones, tricking victims into entering their personal information and making Bitcoin payments. Once the Bitcoin is transferred, it is impossible to reverse the transaction, leaving the victims defrauded. This method leverages the trust people place in recognized brands and services.

Employment Scams

In employment scams, victims are offered fake jobs and are asked to pay for job-related expenses or training in Bitcoin. Scammers create elaborate job offers with attractive salaries and benefits, convincing victims to invest in the required materials or certifications. In some cases, victims are used as money mules to transfer Bitcoin for the scammer under the guise of job tasks. Once the victims realize the job offer was a scam, they are often left with significant financial losses and, in some cases, may face legal issues for unknowingly participating in money laundering activities.

Ransomware Attacks

Ransomware attacks involve malicious software that encrypts the victim's files, rendering them inaccessible. The attackers then demand a ransom in Bitcoin to decrypt the files and restore access. Victims are often desperate to regain their data, leading them to comply with the ransom demands. However, paying the ransom does not guarantee that the files will be restored, and it encourages further criminal activity. These attacks target individuals, businesses, and even government agencies, causing widespread disruption and financial losses.

Fake Charities and Donations

Scammers create fake charities or fundraising campaigns, soliciting donations in Bitcoin for causes that do not exist. They exploit people's generosity and desire to help others, particularly during times of crisis or natural disasters. These fake charities often have professional-looking websites and emotional stories to convince victims to donate. Once the Bitcoin is transferred, it is difficult to trace, and the scammers disappear with the funds. This method not only defrauds victims but also diverts resources away from legitimate charitable causes.

Artificial Intelligence and Deepfake Videos

Legendary investor Warren Buffett said recently that AI's use in online scams is going to be the biggest "growth industry of all time." Scammers are using AI to create pretending to be business leaders, celebrities, love interests, and even politicians.

Rep. Barbara Lee (D-Calif.) criticized Elon Musk for sharing a deepfake video that impersonates Vice President Kamala Harris and mocks her and President Biden. The video, posted on social platform X, falsely portrays Harris as calling Biden senile and herself the "ultimate diversity hire." Lee condemned the video as "dangerous" and called for regulations on AI to prevent such misuse.

California Gov. Gavin Newsom also criticized the video, stating that manipulating voices in this manner should be illegal, and he plans to sign a bill to enforce this. Federal regulators are increasingly looking to regulate deepfake technology, especially in political contexts, with the Federal Communications Commission advancing a proposal to require AI disclosure in ads. The Harris campaign responded by emphasizing that Americans want real leadership, not "fake, manipulated lies."

What is a Deepfake Video and How is AI Involved in Scams

A deepfake video is a synthetic media in which a person in an existing image or video is replaced with someone else's likeness. Utilizing artificial intelligence, particularly deep learning algorithms, these videos can be highly convincing, making it difficult to discern real from fake. AI is involved in scams by creating these deepfakes to impersonate celebrities, politicians, or business leaders, thus lending credibility to fraudu lent schemes. For example, a scammer might create a deepfake video of a well-known personality endorsing a dubious investment, thereby deceiving individuals into parting with their money.

How it is Used in Investment Scams

Deepfake technology is also exploited in investment scams, where fraudsters create videos of famous entrepreneurs, such as Elon Musk, promoting fake investment opportunities. These videos appear highly realistic, convincing unsuspecting individuals to invest in fraudulent schemes. For example, a deepfake video of Elon Musk endorsing a cryptocurrency could lead to massive financial losses for investors. News reports have documented such scams where deepfakes are used to trick people into believing in false endorsements.

Financial regulators are increasingly responding to the rise of deepfake videos in the investment sector by encouraging institutions to incorporate robust cybersecurity measures into their operations. Key actions include training employees to identify deepfakes by looking for telltale signs like unusual skin tones, inconsistent shadows, and lip-synch errors. Regulators also advocate for the evaluation and adoption of AI-based technologies that detect fraudulent deepfakes, using tools that verify image authenticity and customer identities through facial biometrics.

Moreover, regulators are urging the deployment of multifactor authentication across financial networks, with an emphasis on enhanced measures such as issuing physical tokens for authentication. The use of biometrics, like fingerprints or facial recognition, is recommended for secure and convenient customer verification, though institutions must remain compliant with state laws governing biometric data. Finally, regulators stress the importance of educating customers on how to protect their data, as a proactive step in safeguarding against deepfake-related fraud.

How it is Used in Romance Scams

In romance scams, deepfakes are used to create fake video calls and messages, making the scammer appear as someone they are not. By using AI to generate videos of attractive individuals expressing love and affection, scammers can emotionally manipulate their victims. These deepfakes enhance the believability of the scam, making victims more likely to send money or personal information. Reports have shown an increase in deepfake-enabled romance scams, where victims are deceived into long-term relationships with non-existent individuals.

Key Emotional Manipulation Tactics in Romance Scams:

1. **Creating a Rapid Emotional Connection:** Scammers quickly establish an intense emotional bond with the victim, often declaring love or deep affection early in the interaction. This tactic is designed to make the victim feel special, loved, and valued, creating a sense of urgency in the relationship. The speed at which the relationship progresses can cloud the victim's judgment and reduce their skepticism.
2. **Building Trust and Dependency:** Over time, scammers work to build a deep level of trust, sharing fabricated personal stories, and even creating a sense of mutual reliance. Victims are often led to believe that the scammer is their confidant and soulmate, making them more willing to comply with requests for money or personal information. The scammer may also create scenarios where the victim feels responsible for the scammer's well-being, further deepening the emotional dependency.
3. **Exploiting Sympathy and Guilt:** Scammers frequently use sob stories or emergencies to elicit sympathy from the victim. They may claim to be in financial trouble, facing a medical crisis, or dealing with a personal tragedy. These fabricated scenarios are designed to trigger the victim's compassion and guilt, making them more likely to offer financial assistance or other forms of help.
4. **Isolating the Victim:** To maintain control, scammers often attempt to isolate the victim from their friends and family. They may discourage the victim from sharing details of the

relationship with others, warning that outsiders won’t understand or might try to sabotage the relationship. This isolation prevents the victim from receiving outside perspectives that could alert them to the scam.

The Role of Deepfakes in Enhancing Emotional Manipulation:

Deepfake technology has taken the tactics used in romance scams to a new level by making the deception even more convincing and difficult to detect. Deepfakes involve the creation of realistic but fabricated images, videos, or audio, allowing scammers to present a more authentic-seeming identity to their victims.

1. **Creating Convincing Visual Evidence:** Deepfakes enable scammers to produce videos or images that appear to show the scammer in real-life scenarios, interacting with the victim in a way that text or static photos cannot. For example, a scammer could send a deepfake video of "themselves" speaking directly to the victim, reinforcing the illusion of a genuine connection. This visual authenticity makes it harder for victims to doubt the scammer’s identity.
2. **Enhancing the Illusion of a Real Relationship:** By using deepfakes, scammers can maintain the illusion of a consistent and believable persona. For instance, if the scammer claims to be a particular individual, deepfake technology can create a video or audio message that seems to match that person’s appearance and voice. This level of detail deepens the emotional bond, as the victim feels they are truly interacting with a real person, not just a faceless entity online.
3. **Amplifying the Impact of Manipulative Scenarios:** Deepfakes can be used to create dramatic, emotionally charged scenarios that elicit strong reactions from the victim. For example, a scammer might send a deepfake video showing themselves in a dangerous situation, pleading for help. The emotional impact of seeing a loved one in distress, even if fabricated, can push the victim to act impulsively, often leading to financial loss or other forms of exploitation.

   Fake Elon Musk Crypto Investment Scams: Scammers have used deepfake technology to create videos of Elon Musk promoting fake cryptocurrency investments. These scams have led to significant financial losses for victims.

   Politicians and Deepfake Threats: The potential for deepfake technology to disrupt political campaigns is significant. Instances of deepfakes used against politicians have already surfaced, with concerns about their impact on future elections. American Bar provides insights into how deepfakes are expected to influence upcoming elections in this article.

Deepfake videos represent a significant advancement in digital technology, utilizing artificial intelligence and machine learning to create or alter video content so convincingly that it becomes difficult to distinguish real from fabricated. This technology synthesizes human images and voices, enabling the creation of video clips that show people doing or saying things they never did. Originally developed for benign purposes like film production and personal entertainment, deepfakes have rapidly morphed into tools for misinformation, harassment, and fraud.

The dangers of deepfake videos are profound and multifaceted. They pose serious threats to personal reputation, as fabricated videos can spread false information or damaging allegations about individuals, potentially leading to personal and professional ruin. On a larger scale, deepfakes can be used to create false narratives that inflame public opinion, manipulate elections, or even incite violence. For example, a convincingly altered video could show a political leader making inflammatory statements they never actually made, potentially leading to international diplomatic incidents.

Given the risks associated with deepfakes, it's crucial for individuals and organizations to develop skills to spot them. While the technology is sophisticated, certain imperfections can help viewers identify fakes:

1. **Unnatural Movement**: Look for irregularities in facial movements or expressions. In many deepfakes, the blink rate or subtle facial movements are off, or there may be anomalies in how the eyes, mouth, or other features move.
2. **Inconsistent Lighting and Shadows**: Deepfakes often struggle with maintaining consistent lighting and shadows, especially when elements from different sources are combined. Discrepancies in shadow direction or lighting quality can be telltale signs.
3. **Poor Lip Syncing**: In videos where the person is speaking, mismatches between the spoken words and the movement of the lips can be an indicator.
4. **Audio Irregularities**: Changes in the tone or quality of the voice that don’t match usual patterns can be a red flag, especially if the audio sounds flat or emotionless.
5. **Using Reliable Sources**: Always check the source of a video. Trusted and verifiable sources are less likely to distribute deepfakes.

In addition to personal vigilance, technological solutions are also being developed to detect deepfakes. Companies and researchers are working on AI-driven tools that can spot signs of digital tampering that might be invisible to the human eye. Public awareness campaigns and education about digital media literacy can also empower individuals to critically assess the content they consume, reducing the impact of deepfakes. As this technology evolves, a multi-faceted approach involving technology, regulation, and education will be essential to mitigate the threats posed by deepfake videos.

Legal Implications of Deepfakes: Current Laws and Proposed Regulations

Deepfakes, which involve the use of artificial intelligence to create realistic but fabricated images, videos, or audio, have raised significant legal and ethical concerns worldwide. As the technology becomes more sophisticated, its potential for misuse has prompted governments to consider and implement legal measures to address the challenges it poses.

Current Laws Governing Deepfakes

In many countries, existing laws that were not originally designed with deepfakes in mind are being adapted to cover their misuse. For instance, in the United States, there is no federal law specifically targeting deepfakes, but several states have enacted their own laws. For example:

- **California** passed a law in 2019 that makes it illegal to create or distribute deepfake videos intended to influence an election within 60 days of the election date. Another law in California allows victims of non-consensual deepfake pornography to sue for damages.
- **Virginia** also criminalized the use of deepfake technology to create and distribute non-consensual pornographic material, treating it as a form of sexual harassment.

At the federal level, the **Malicious Deep Fake Prohibition Act** was introduced in Congress in 2018, aiming to criminalize the creation and distribution of deepfakes intended to harm, defraud, or deceive. However, it has not yet been passed into law.

In the European Union, the General Data Protection Regulation (GDPR) provides some protection against deepfakes, particularly in cases where personal data is used without consent. However, the regulation was not specifically designed to address the nuances of deepfake technology.

Proposed Regulations and Future Considerations

Given the growing concern over deepfakes, there are several proposed regulations and legislative efforts underway:

- **The United Kingdom** is considering new legislation as part of its Online Safety Bill, which would impose duties on tech companies to tackle harmful content, including deepfakes. This bill could require platforms to remove deepfake content swiftly and to implement stronger verification processes for uploaded media.
- **The European Union** has proposed the **Digital Services Act (DSA)**, which, if passed, would impose stricter regulations on online platforms, requiring them to take down illegal content, including deepfakes, more quickly. The DSA would also mandate transparency in algorithms used by these platforms, potentially addressing how deepfakes are disseminated.
- **Australia** is also exploring new laws to combat the use of deepfakes, particularly in the context of image-based abuse. The country's existing laws on cyberbullying and online harassment could be expanded to include deepfakes.

Internationally, there is a growing recognition of the need for coordinated efforts to combat the misuse of deepfakes. Organizations like the **United Nations** and the **Council of Europe** are beginning to discuss the implications of deepfake technology and the necessity for global standards and cooperation.

Challenges and Enforcement

One of the major challenges in regulating deepfakes is the difficulty in detecting and proving that a deepfake has been used maliciously. The rapid advancement of AI technology means that deepfakes are becoming increasingly realistic and harder to identify. Additionally, the global nature of the internet complicates enforcement, as content can be created in one jurisdiction and distributed in another, making it difficult to hold perpetrators accountable.

Another challenge is balancing regulation with freedom of expression. While there is a clear need to prevent the harmful use of deepfakes, there is also a risk that overly broad or restrictive laws could stifle legitimate uses of the technology, such as in satire, art, or political commentary.

Online Scams and the 2024 Presidential Election

Deepfake Technology

Deepfake technology poses a significant threat to the integrity of the 2024 Presidential Election. This advanced AI technique allows for the creation of highly realistic videos in which individuals appear to say or do things they never did. In the political arena, deepfakes can be used to spread misinformation, discredit candidates, and manipulate public opinion. For instance, a deepfake video showing a candidate making inflammatory statements could go viral, leading to widespread confusion and potentially influencing voters. The ability of deepfakes to undermine trust in visual media is a serious concern for upcoming elections (The Verge, Forbes).

The increasing use of AI tools like deepfakes is causing significant concerns regarding their potential impact on elections. In India, deepfake creator Divyendra Singh Jadoun has reported a surge in requests from politicians to create fake media, including unethical deepfakes designed to defame opponents or manipulate voter perceptions. This surge illustrates how AI-generated content can be weaponized in political campaigns, raising fears about its potential to distort the democratic process.

The rise of AI-powered tools makes it easier for not just state actors but also smaller, less-resourced groups to create sophisticated fake media. This democratization of AI means that false content, such as fabricated videos or audio clips, can spread rapidly on social media, potentially misleading voters on a large scale. In response, some regions, like certain U.S. states, have begun enacting laws to penalize the creation and distribution of such deceptive content, although these measures vary widely and may not be enough to counteract the rapid spread of misinformation.

Global experts, including those from the Department of Homeland Security, have warned about the dangers of AI-enhanced disinformation campaigns, particularly as they pertain to upcoming elections. The potential for AI to generate convincing fake content that could sway voter opinions underscores the urgency of developing better detection tools and more robust regulatory frameworks to mitigate these risks.

In the absence of comprehensive regulations, efforts to control the spread of AI-generated political content have largely fallen on tech companies and individuals like Jadoun, who must navigate the ethical implications of their work. As AI tools become more advanced and accessible, the risk of AI-driven election interference becomes a pressing concern that could have profound implications for the integrity of democratic processes worldwide.

Given the rapid evolution of these technologies, their impact on future elections could be significant, potentially undermining trust in electoral outcomes and eroding public confidence in democratic institutions. As such, there is a critical need for both regulatory action and public awareness to ensure that elections remain free and fair in the age of AI.

As policymakers and regulators across Brussels and Washington rush to draft legislation aimed at restricting the use of AI-powered audio, images, and videos during political campaigns, a significant regulatory gap is becoming evident. The European Union's key legislation, the AI Act, will not be implemented until after the June parliamentary elections. Similarly, in the U.S., bipartisan efforts to prohibit the false depiction of federal candidates using AI technology are unlikely to result in new laws before the November elections.

Election Security Measures

A recent scandal involving a deepfake of President Joe Biden highlights growing concerns about AI-generated misinformation in elections. The deepfake, created by a New Orleans street magician and used in a New Hampshire robocall, urged voters not to participate in the primary. This incident has prompted many states to introduce and pass laws banning deepfakes in elections. Since January of last year, 41 states have introduced such bans, and eight have enacted them, joining California and Texas, which passed similar laws in 2019.

However, these laws vary in approach and effectiveness, often balancing the need to prevent election interference with the protection of free speech. For example, Wisconsin and New Mexico require disclaimers on AI-generated content, while Georgia’s law, which also includes carveouts for satire and journalism, criminalizes certain uses of deepfakes around elections.

Experts warn that while these laws focus on deepfakes of politicians, other AI-related threats, like AI-generated misinformation through mass texting or voice cloning, remain under-addressed. As we head into the upcoming election, there is concern that these laws may not fully cover the evolving risks that AI poses to democracy.

Other

In addition to deepfake technology, other online scams are expected to play a role in the 2024 Presidential Election. These scams include phishing attacks designed to steal sensitive information from campaign staff and voters, as well as fake donation schemes that trick supporters into giving money to fraudulent causes (CNN). Another prevalent scam involves selling fake political merchandise, such as counterfeit campaign hats, shirts, and memorabilia. These scams not only divert funds from legitimate campaigns but also deceive voters into supporting fictitious entities. Past elections have seen similar tactics, and it's likely these will continue and evolve with new technologies.

Fake Donations

Fake donation scams are particularly insidious as they exploit the goodwill of supporters. Scammers set up websites that mimic official campaign donation pages, tricking individuals into donating to fraudulent accounts. These scams can significantly harm a candidate's fundraising efforts by diverting potential funds. Additionally, they can lead to a loss of trust among supporters who discover that their contributions never reached their intended destination. During the 2020 election, numerous reports surfaced of fake donation sites exploiting both major parties.

Fake Merchandise

Another scam that can impact the election involves the sale of fake merchandise. Fraudsters create online stores selling counterfeit campaign items, such as T-shirts, hats, and buttons, often at a lower price than official merchandise. This not only results in financial losses for the campaign but also misleads supporters who believe they are purchasing authentic products. Moreover, these counterfeit items are often of poor quality, reflecting badly on the campaign they are supposed to support. Past elections have seen a surge in such scams, with fake merchandise flooding online marketplaces.

The Rise of AI Image Generation

AI image generation technology, while revolutionary in creative fields, is increasingly being exploited by scammers. Companies like Microsoft, OpenAI, and Google have developed powerful AI tools capable of creating highly realistic images from simple text prompts. Unfortunately, this has opened the door for malicious actors to use AI-generated visuals in fraudulent schemes, such as creating fake identities, phishing attempts, and counterfeit profiles on social media. The ease with which these AI-generated images can mimic real people or scenarios has heightened the need for vigilance and security measures to combat the growing threat of AI-powered scams.

Key Growth Drivers and Market Segmentation

AI Image Generator Market Growth Factors (AR & VR)

The rapid adoption of Augmented Reality (AR) and Virtual Reality (VR) technologies is a major driver for the AI image generator market. These technologies rely heavily on realistic, data-driven, and immersive visuals, which AI image generators can create efficiently. From gaming to automotive design, AI-generated images enhance the visual richness of AR and VR experiences by producing intricate 3D environments, lifelike characters, and dynamic simulations. As industries like healthcare, education, and entertainment increasingly integrate AR and VR, the demand for high-quality AI-generated visuals will continue to grow, making these technologies key contributors to the market's expansion.

Global AI Image Generator Market Share

The global AI image generator market is segmented into several end-user categories, with the advertising sector dominating due to its need for streamlined creative processes. AI-generated images help advertisers cut costs while producing engaging, customized visuals that enhance ad campaigns in an increasingly visual digital landscape. Other sectors like healthcare, gaming, fashion, and e-commerce also play a significant role, utilizing AI for generating dynamic content, improving user experiences, and staying competitive. The fashion industry, in particular, is poised for significant growth, as brands embrace AI tools to quickly adapt to evolving trends and create cost-effective, personalized visuals.

Regional Insights

North America leads the global AI image generator market, driven by its advanced technological infrastructure and the presence of key industry players. The U.S. and Canada host top AI research institutions and tech companies that fuel innovation in AI-generated content for healthcare, entertainment, and advertising. Asia Pacific is also experiencing rapid growth, with China, Japan, and India emerging as key players due to their expanding tech landscapes and increasing digital adoption. In Europe, the demand for AI-driven solutions spans across industries such as healthcare, automotive, and gaming, while South America and the Middle East & Africa are seeing nascent yet promising developments in AI adoption.

Key Industry Players & Development

The AI image generator market is highly competitive, with key players such as Adobe, OpenAI, Stability AI, and VanceAI continuously pushing the boundaries of innovation. Companies are enhancing their product portfolios by introducing advanced AI tools that automate content creation and offer customization options for users. Many of these organizations are also expanding their reach through collaborations, acquisitions, and partnerships, strengthening their positions in the market. Notable developments include the launch of DALL-E 3 by OpenAI, Adobe's Firefly AI tool, and Stability AI's open-source StableStudio, all of which have set new standards in AI-driven image generation.

Recent developments in the AI image generator market include significant advancements in text-to-image technologies. OpenAI's DALL-E 3 has introduced high-quality image generation based on natural language prompts, while Adobe's Firefly provides users without graphic design skills the ability to create sophisticated images and text effects. Companies like Runway AI have also made strides with tools such as Gen-2, which allows for the creation of short video clips from text prompts. These developments showcase the growing capabilities of AI tools, which are becoming increasingly accessible to a wider audience, driving further innovation in the industry.

Growth of Image Generation Startups

The growth of AI image generation has been driven by significant investments from both startups and big tech giants, as the demand for innovative and scalable solutions increases across various industries. Startups like Runway, Tavus, and Kittl have gained traction by offering enterprise-focused tools for marketing, sales, and e-commerce businesses, securing millions in funding to develop their AI-powered visual media solutions. With AI models tailored to specific business needs, these startups help companies streamline workflows, such as generating product shots or personalized videos. At the same time, larger corporations like Apple and Google have also made strides in AI-generated content, with features like Apple's Intelligence and Google's Imagen 3 pushing the boundaries of image creation.

However, while this innovation brings vast opportunities, it has also ignited legal and ethical debates, particularly regarding the use of copyrighted content in training AI models. Companies such as Stability AI and Midjourney face legal challenges from artists who claim their work was used without consent. In contrast, startups like BRIA are adopting a licensing model that ensures content creators are compensated, similar to how Spotify compensates artists for their music. This approach not only supports a fairer ecosystem for creators but also addresses concerns about the potential misuse of AI-generated images in areas like advertising and politics. As AI image generation continues to evolve, balancing innovation with responsible use will be crucial.

The Progression of AI Image Generation Over the Past Years

AI image generation has made significant strides in recent years, transforming from rudimentary algorithms producing crude visuals to sophisticated models like OpenAI's DALL-E 3 and Google's Imagen 2. Early AI-generated images often struggled with realism, producing bizarre or distorted results. However, modern advancements in deep learning have dramatically improved the quality, allowing AI to generate hyper-realistic images that are nearly indistinguishable from real photographs. The continued evolution of AI in this field shows immense potential for both creative applications and, unfortunately, deceptive practices.

Microsoft

Microsoft's AI image generation is powered by DALL-E 3, OpenAI's most advanced model, accessible for free through its Image Creator and Copilot platforms. This integration allows users to seamlessly generate high-quality images while interacting with Microsoft's AI chatbot, offering a convenient and efficient way to combine text and image creation in one place. Whether through Image Creator's standalone site or within Copilot, users can conversationally generate images that align with their project needs without needing a paid subscription, making AI-powered creativity accessible to all.

OpenAI

OpenAI's DALL-E 3 is at the forefront of AI image generation, providing users with highly realistic and detailed visuals based on specific prompts. However, access to DALL-E 3 requires a subscription to ChatGPT Plus, priced at $20 per month. Subscribers can generate stunning images directly within ChatGPT, making it easy to incorporate both text and visuals into their projects. DALL-E 3 also features advanced editing tools that allow users to refine their images further through conversational prompts, making it a powerful tool for scammers who need customized, high-quality visuals.

Google

Google's AI image generation, integrated into Gemini, utilizes the Imagen 2 model to produce realistic images. The platform's seamless connection with Google Search allows users to generate and verify images within the same interface, offering four simultaneous outputs per prompt. Gemini's user-friendly design mimics the familiar Google interface, making it intuitive for users to navigate and generate images while ensuring the reliability of the AI's output through integrated search verification, bridging the gap between creativity and accurate information.

The Legality of AI-Generated Images

The rise of AI image generation has sparked numerous legal and ethical debates. Governing the use of AI-generated images involves navigating complex issues such as intellectual property, consent, and deepfake regulation. Many countries have yet to establish comprehensive laws surrounding AI images, but some have introduced legislation targeting the misuse of AI for creating deceptive or harmful content, like deepfakes. As AI-generated visuals become more prevalent, legal frameworks will need to evolve to ensure accountability, protect creators' rights, and prevent malicious use.

A new bill introduced in the US Congress aims to force AI companies to disclose the copyrighted material used to train their generative AI models. The legislation, spearheaded by Congressman Adam Schiff, mandates that companies submit their training datasets, which include copyrighted works like music, images, and text, to the Register of Copyrights at least 30 days before launching new AI tools. While the bill doesn't prohibit the use of copyrighted material for training, it imposes stricter disclosure requirements, with potential financial penalties for non-compliance. This initiative reflects growing concerns from lawmakers, artists, and industry leaders about the potential misuse of creative works by AI firms, especially given the ongoing legal battles facing companies like OpenAI, which are accused of infringing on copyright through the use of such materials in their AI tools.

The bill has received strong support from various entertainment industry organizations, underscoring the need to protect intellectual property rights in the era of AI. As generative AI technologies expand their capabilities, the question of whether their reliance on copyrighted content falls under "fair use" remains contentious. Prominent AI companies, including OpenAI, argue that copyright law does not explicitly prohibit the training of AI with such works, though this legal stance is being tested in numerous lawsuits. The outcome of these cases could have profound implications for both the AI industry and the livelihoods of artists, as tensions rise over the role of AI in creative fields.

Tips on How to Detect AI-Generated Images

While AI-generated images can be highly convincing, certain markers can help you spot them. Look for anomalies in symmetry, lighting, or details that seem unnatural, such as distorted hands or facial features. Overly smooth textures, inconsistencies in shadows, and a lack of fine detail are also telltale signs. Trust your instincts—if something looks too perfect or slightly off, it could be AI-generated. Scrutinizing small details can often reveal the subtle glitches typical of AI creations.

Tools Available to Detect AI-Generated Images

As AI image generation has progressed, so too have the tools designed to detect them. Platforms such as **"AI or Not"** and **"Deepware"** specialize in analyzing images for signs of AI involvement. These tools use reverse image search, facial recognition inconsistencies, and deep learning algorithms to determine whether an image is AI-generated. These detection tools are essential for maintaining authenticity in digital content and preventing the spread of AI-based misinformation.

Exploring the Evolving Landscape of Scams: Insights from Our 2024 Surveys

In July-August 2024, we conducted two detailed surveys to uncover insights into the growing landscape of scams. The first survey, focused on online scams in general, gathered responses from 500 individuals and provided valuable data on the types of scams, victim experiences, and their consequences. The second survey, with 1,000 participants, delved into the emerging role of AI in online scams, including the use of deepfake videos and AI-generated audio. Both surveys were conducted to better understand how scams are evolving and their impact on people’s lives. The results reflect the latest trends and behaviors and offer a timely snapshot of the threats individuals face online.

Key Findings

Popular Platforms for Scams
According to our online scam survey of 500 participants, social media continues to be a major platform where scams occur. Facebook was the leading platform, with 27.91% of respondents reporting they encountered scams on this platform. Other platforms, such as Instagram

(12.85%) and WhatsApp (12.45%), also saw significant scam activity. Interestingly, dating apps like Tinder and Bumble saw lower percentages but are still notable, with Tinder at 1.41% and Bumble at 1.20% ￼.

Common Payment Methods Used by Scammers
Cryptocurrency remains the most common payment method used by scammers, with 26.99% of participants indicating they had sent payments via Bitcoin or Ethereum. Gift cards were also widely used (43.35%), and wire transfers or bank transfers accounted for 25.15%.

Reporting Scams
Only 19.67% of participants reported their scam experiences to the Federal Trade Commission (FTC), despite 80.33% of respondents having been scammed. This highlights a potential gap in reporting, which may be due to the complexity of reporting systems or victims not knowing where to file a report.

Consequences of Scams
The impact of scams extends beyond financial losses. Nearly half (47.41%) of respondents faced financial hardship, while 56.52% reported emotional distress, and 28.99% experienced relationship strain. This indicates that scams leave lasting psychological and social impacts in addition to the monetary damage￼.

Familiarity with AI and Deepfake Videos
In our AI-focused survey with 1,000 respondents, 39.18% of respondents were moderately familiar with the concept of deepfake videos, and 31.19% had encountered a deepfake video online. This suggests that while awareness is growing, a significant portion of the population may still be vulnerable to AI-powered scams.

Victimization by AI-Driven Scams
A significant 38.87% of respondents reported that they or someone they knew had fallen victim to an online scam involving AI technologies such as deepfake videos or AI-generated audio. The most common types of scams related to AI were romance scams (64.13%) and phishing attempts (21.28%), with fewer incidences of investment (6.38%) or political scams (2.43%)￼.

Financial Loss from AI Scams
Nearly half of those scammed by AI-driven techniques experienced financial losses. The survey revealed that 47.56% faced no financial loss, but 25.71% lost over $5,000 due to these scams. This underscores the high stakes involved in AI scams.

Confidence in Detecting Deepfakes
Although a significant portion of respondents are concerned about AI-based scams, only 12.24% were aware of tools to detect deepfakes, and just over half (50.93%) expressed low confidence in their ability to identify deepfake videos. This reflects a growing need for educational tools and resources to help people identify AI-generated content.

Concerns About AI in Politics

The survey also highlighted concerns about the potential misuse of AI, particularly in the political sphere. Around 31.42% of participants were extremely concerned about deepfakes being used in political campaigns, while 67.21% believed that deepfake videos could significantly or extremely influence voter decisions in elections￼.

Rise of Sextortion Scams

Sextortion scams have seen a troubling rise, exploiting the intimate vulnerabilities of individuals to extort money or personal information. These scams typically begin with scammers gaining access to explicit photos or videos of the victim, often through social media platforms like Facebook and Instagram. Once they have compromising material, the scammers threaten to release it publicly unless the victim pays a ransom. This form of exploitation has led to severe psychological distress and, tragically, in some cases, even suicide. A poignant example is the case covered by CBS News, where victims were driven to extreme actions due to the fear and shame instilled by these criminals .

The impact of sextortion scams is widespread and devastating. Platforms like Meta (Facebook and Instagram) are increasingly cracking down on these malicious activities, yet the problem persists. According to a Bloomberg report, there has been a notable increase in teenage suicides linked to sextortion, highlighting the critical need for awareness and preventive measures . These scams not only destroy lives but also instill a pervasive sense of insecurity and fear among social media users. It is crucial to educate individuals about the risks and encourage them to report suspicious activities to help mitigate the rise of such exploitative scams.

The tragic story of Jordan DeMay highlights the dark side of social media and the vulnerability of teenagers to online threats. Jordan, a popular high school athlete, was manipulated into sending a compromising photo of himself to someone he believed was a teenage girl. This quickly escalated into a nightmare of sextortion, where he was blackmailed for money with threats of sharing the photo publicly and sending it to his loved ones. Despite his efforts to comply by paying the demanded sum, the harassment continued, leading him to a state of despair. This severe emotional distress culminated in his suicide, leaving behind a devastated community and raising urgent questions about the safety mechanisms of social media platforms and the predatory nature of online criminals.

These romance fraud schemes are not thought to exclusively target minors, as reports indicate that many young adults are similarly affected. Among minors, male teenagers are the most likely to be targeted in financial sextortion cases.

Data Breach and Online Scam

10 Billion Passwords Leaked: Largest Password Leak of All-Time

In July 2024, Cybernews researchers uncovered what appears to be the largest password compilation ever, dubbed RockYou2024 leak. This colossal dataset, containing nearly 10 billion unique plaintext passwords, poses a significant threat to online security. With the data sourced from a variety of old and new breaches, the potential for credential stuffing attacks and other cyber threats has never been higher. The RockYou2024 leak has set a new record with 9,948,575,739 unique plaintext passwords exposed. This dataset surpasses the previous record held by RockYou2021, which contained 8.4 billion passwords. The sheer size of RockYou2024 highlights the growing volume of data breaches and the increasing sophistication of cybercriminals in aggregating such vast amounts of sensitive information.

The compilation of RockYou2024 is not an isolated incident but rather an expansion of previous leaks. It underscores the persistent threat posed by cybercriminals who continually scour the internet for new data leaks. This new dataset includes an additional 1.5 billion passwords collected from 2021 to 2024, emphasizing the ongoing risk and the need for heightened cybersecurity measures.

The RockYou2024 leak, which exposed billions of passwords, is likely to have significant long-term effects on cybersecurity practices and user behavior. This massive data breach underscores the vulnerabilities in current password management practices and highlights the need for more robust security measures across the digital landscape.

One of the key impacts on cybersecurity practices will likely be the increased adoption of stronger authentication methods. The scale of the RockYou2024 leak could push companies and organizations to move beyond traditional passwords, implementing multifactor authentication (MFA), biometrics, and passwordless systems. Additionally, there may be a greater investment in AI-driven security tools that can detect and respond to unusual login behaviors, making it more challenging for attackers to exploit leaked credentials. Moreover, the breach could lead to a surge in the use of password management tools that generate and store complex, unique passwords. Companies might promote or mandate the use of these tools among employees to prevent future breaches. Regulatory bodies may also introduce stricter guidelines on how companies handle and protect user data, potentially leading to new compliance requirements and regular security audits.

In terms of everyday user behavior, the leak is likely to increase awareness of cybersecurity, leading users to adopt more cautious practices online. This might include creating strong, unique passwords and changing them regularly, as well as embracing multifactor authentication to protect their accounts. However, the leak could also contribute to a growing skepticism towards online platforms that do not prioritize security, driving users toward services known for robust cybersecurity measures. Conversely, there is a risk of cybersecurity fatigue among users, who may feel overwhelmed by the constant need to update passwords and manage security settings. This fatigue could lead to complacency, making users more vulnerable to future attacks.

Understanding Credential Stuffing Attacks

Credential stuffing is a type of cyberattack where attackers use automated tools to try a vast number of username and password combinations to gain unauthorized access to accounts. With nearly 10 billion passwords now available in the RockYou2024 dataset, the risk of credential stuffing attacks has escalated dramatically. These attacks are particularly effective because many users reuse passwords across multiple sites.

Recent credential stuffing attacks have had severe consequences for businesses and individuals alike. High-profile victims like Santander, Ticketmaster, and Advance Auto Parts have experienced significant disruptions due to these attacks. The availability of the RockYou2024 compilation means that any system not adequately protected by robust authentication mechanisms is vulnerable to such intrusions.

One of the most notable trends in credential stuffing is the growing use of automation and artificial intelligence (AI) to enhance the efficiency and effectiveness of these attacks. Attackers are leveraging AI-driven tools that can rapidly test millions of credentials across multiple platforms, significantly increasing their chances of success. These tools can also mimic human behavior, making it more difficult for security systems to detect and block automated login attempts. By adjusting parameters such as login speed and timing, AI-driven bots can evade traditional security measures like rate limiting and CAPTCHA challenges.

Another emerging trend is the shift toward targeting APIs (Application Programming Interfaces) and mobile applications in credential stuffing attacks. APIs, which facilitate the communication between different software applications, often have weaker security controls compared to traditional web interfaces. Attackers are exploiting these vulnerabilities to bypass security measures and gain access to user accounts. Similarly, mobile applications, which may not always implement robust security practices, are becoming prime targets for credential stuffing. Attackers are increasingly focusing on these less protected entry points to infiltrate systems and steal valuable data.

Credential stuffing as a service (CaaS) is another trend that has emerged, making it easier for even less technically skilled attackers to engage in credential stuffing. In this model, cybercriminals offer credential stuffing tools and services for rent or purchase on dark web forums. These services often come with user-friendly interfaces and customer support, allowing individuals with minimal hacking experience to launch sophisticated credential stuffing attacks. CaaS lowers the barrier to entry for cybercriminals, leading to a proliferation of credential stuffing incidents across various industries.

Attackers are also diversifying their attack vectors, moving beyond just targeting well-known platforms like social media sites and financial institutions. Increasingly, they are focusing on smaller websites, online retailers, and subscription-based services, which may have weaker security measures. This trend underscores the importance of robust security practices across all online platforms, regardless of size or industry, as attackers are constantly seeking out the path of least resistance.

As multi-factor authentication (MFA) becomes more widely adopted, attackers are evolving their techniques to bypass this additional layer of security. Some attackers are using phishing attacks to trick users into revealing their MFA codes, while others are exploiting vulnerabilities in MFA implementations, such as intercepting SMS-based codes. Additionally, attackers are increasingly targeting account recovery processes, which may be less protected, to reset passwords and bypass MFA altogether.

Credential stuffing is often combined with other attack methods to increase the likelihood of success. For example, attackers may pair credential stuffing with social engineering techniques, such as phishing, to gather additional information about the victim and improve the accuracy of their attacks. In some cases, credential stuffing is used as a precursor to more targeted attacks, such as spear-phishing or account takeover fraud, where attackers focus on high-value targets like executives or individuals with access to sensitive information.

In response to these evolving techniques, organizations are adopting more sophisticated defense strategies. These include implementing more advanced threat detection systems that use machine learning to identify and block credential stuffing attempts in real-time. Companies are also investing in continuous monitoring of login activities and improving the security of APIs and mobile applications. Additionally, there is a growing emphasis on educating users about the importance of using unique passwords for each account and enabling multi-factor authentication.

5 Tips to Protect Your Passwords

The recent RockYou2024 password leak has significantly heightened the risk of credential stuffing attacks and unauthorized access to personal accounts. In response to these growing threats, solutions like Social Catfish’s Privacy Lock can offer critical protections to help mitigate these risks. An identity protection solution such as Privacy Lock is designed to provide users with advanced security features that protect their online accounts from unauthorized access.

Privacy Lock includes proactive threat monitoring capabilities that can alert users to potential security breaches in real-time. By continuously scanning the web for signs of data breaches and compromised accounts, Privacy Lock can provide timely notifications if any of the user’s credentials appear in leaks like RockYou2024. This early warning system allows users to take immediate action, such as changing their passwords and securing their accounts before attackers can exploit the compromised information. Additionally, Privacy Lock can guide users through the process of updating their security settings and implementing stronger authentication measures to further enhance account protection.

The RockYou2024 password leak represents a significant escalation in the ongoing battle against cyber threats. With nearly 10 billion passwords exposed, the potential for credential stuffing attacks and other malicious activities has never been greater. By understanding the magnitude of this leak, the nature of credential stuffing, and the evolution of such datasets, both individuals and organizations can take informed steps to protect themselves. Implementing robust security measures and staying vigilant are key to safeguarding against the threats posed by this unprecedented data breach.

Online Scams are a Global Crisis

Online scams are a global crisis but America is by far the most targeted nation due to its affluence and reliance on technology. According to the FBI Internet Crime Report from 2023, Americans filed 521,652 complaints, while the next 19 most impacted nations filed 315,335 complaints combined.

Where Do Online Scams Originate From?

Pig Butchering Scams from Southeast Asia

Online scams, particularly those involving cryptocurrency, often originate from regions with lax regulatory frameworks and limited law enforcement reach. Southeast Asia, particularly countries like Thailand and Myanmar, has become a hotspot for these scams. Criminal organizations, often operating with the tacit approval or under the radar of local authorities, use these regions as bases for their operations. These scams are not just isolated incidents but part of a broader network of organized crime that takes advantage of weak regulatory environments to perpetrate fraud on a global scale.

One of the most notorious types of online scams originating from Southeast Asia is known as "pig butchering." This scam involves long-term social engineering, where scammers build trust with their victims over weeks or months before convincing them to invest in fraudulent cryptocurrency schemes. The funds are then laundered through complex networks of cryptocurrency wallets, making it challenging for authorities to trace the money or bring the perpetrators to justice. These scams often involve sophisticated layering techniques, where stolen funds are mixed with legitimate transactions to obscure their origins.

The involvement of high-profile individuals and businesses in these scams further complicates the situation. For instance, the investigation into Chinese businessman Wang Yicheng, who has close ties with Thai law enforcement and political elites, revealed that his cryptocurrency account received millions of dollars linked to pig-butchering scams. This account, held at the world’s largest crypto exchange, Binance, was used as a node in a money laundering network, illustrating the deep connections between these criminal activities and legitimate financial institutions.

The global reach of these scams is facilitated by the widespread use of digital currencies and the internet. Victims, often located in different countries from the perpetrators, are lured into these scams through fake websites and social media profiles that appear legitimate. The anonymity provided by cryptocurrencies like Bitcoin makes it easier for scammers to operate across borders without fear of immediate detection or reprisal. This transnational nature of the crimes makes it difficult for any single country to combat these scams effectively.

Moreover, the role of corrupt or complicit local authorities cannot be overlooked. In some cases, as in Thailand, local elites and law enforcement officials have been found to have connections with the individuals behind these scams. This creates a layer of protection for the scammers, making it even harder for international law enforcement agencies to intervene. The situation is further exacerbated by the involvement of powerful criminal organizations, such as the 14K Triad, which have been linked to these scams and operate with near impunity in some regions.

Efforts to combat these scams have been met with mixed results. While there have been crackdowns and arrests, such as the Thai police’s operation against a significant pig-butchering scam with the help of Binance, these actions are often too late to recover the stolen funds or provide justice for the victims. The sophisticated nature of these operations, combined with the complicity of local authorities, means that even successful interventions only scratch the surface of the broader problem.

The human cost of these scams is significant, with many victims losing their life savings and suffering severe emotional distress. Some, like the 71-year-old California man who lost $2.7 million, are left devastated and unable to recover from the financial and psychological impact. As these scams continue to evolve and become more sophisticated, it is crucial for global cooperation and more robust regulatory frameworks to combat the growing threat of online fraud and bring those responsible to justice.

Cybercrimes Associated with North Korea

Cybercrimes are becoming more and more prevalent in North Korea. The U.S. Justice Department has taken actions to disrupt revenue generation efforts by North Korea through illicit

IT worker schemes. The IT workers used stolen U.S. identities to infiltrate U.S. companies. These IT workers were sent by the North Korean government to carry out the act globally.

The workers posed as American citizens in remote positions, defrauding over 300 U.S. companies and raising millions of dollars in revenue for North Korea. This was achieved through U.S. citizen Christina Chapman and Ukrainian national Oleksandr Didenko, creating fake accounts and operating laptop farms where overseas workers appeared as if they were working in the U.S. Chapman and her co-conspirators also laundered money and defrauded U.S. companies to generate illicit income for North Korea.

In another crime, Federal prosecutors have charged Christina Marie Chapman, 49, from Arizona, for helping North Korean nationals obtain IT jobs with U.S. Fortune 500 companies, earning at least $6.8 million for North Korea between October 2020 and October 2023. The North Korean workers, linked to Pyongyang’s Munitions Industry Department, spied for the regime and infiltrated companies across various industries, including a Detroit car manufacturer and a Silicon Valley tech firm. Authorities also charged Ukrainian national Oleksandr Didenko, who allegedly facilitated North Korean remote work by managing up to 871 proxy identities and operating a platform that rented out accounts and credit cards.

Chapman and Didenko set up "laptop farms" within the U.S. to facilitate remote access by North Korean workers who used fake American identities. FBI raids uncovered over 90 computers at Chapman's Arizona home, affecting more than 300 U.S. companies. The pair's operations were part of a broader North Korean strategy to bypass economic sanctions, fund weapons programs, and conduct cyber espionage. Chapman faces up to 97 years in prison, and Didenko faces up to 67 years if convicted.

The next crime features a North Korean IT worker scam that has been targeting U.S. companies like KnowBe4. Despite rigorous hiring practices, including multiple video interviews and background checks, KnowBe4 inadvertently hired a North Korean worker who had stolen a U.S. identity and used AI tools to manipulate his appearance. The company's security team quickly detected suspicious activity on the new employee's laptop, preventing him from accessing their systems or compromising any data, though he did attempt to load malware. The incident underscores the sophistication of North Korean workers in evading detection and securing remote jobs to funnel money to the regime while posing security risks to U.S. companies.

KnowBe4's CEO, Stu Sjouwerman, openly addressed the breach, highlighting the difficulty even security-focused companies face in preventing such threats. He stressed that if it can happen to KnowBe4, it can happen to almost anyone. The company is now recommending stricter vetting processes, including conducting all remote interviews with cameras on and only shipping company equipment to verified addresses or UPS locations. The FBI is investigating the incident as it raises concerns about insider threats, particularly from foreign entities using AI to infiltrate American companies

Another example of cybercrime involved a North Korean hacking group known as Kimsuky exploiting poorly configured email security protocols, particularly flaws in Domain-based Message Authentication, Reporting, and Conformance (DMARC), to carry out sophisticated phishing attacks. Targeting academic institutions, think tanks, journalists, and nonprofits, Kimsuky uses phishing emails disguised as legitimate communications. Once they establish contact, the hackers send follow-up emails with malicious links and attachments to steal sensitive information. In one instance, a hacker posing as a journalist seeking comments on geopolitical issues manipulated email configurations to redirect responses to a North Korean-controlled account. The advisory from the State Department, FBI, and NSA urges organizations to update their DMARC settings to prevent these attacks.

Kimsuky, believed to operate under North Korea's military intelligence directorate, has been active since at least 2012 and is known for stealing data to provide valuable geopolitical insights to the regime. The group supports North Korea's nuclear weapons program, partly funded through covert cryptocurrency transactions. U.S. assessments suggest that North Korean cyber operations, including cryptocurrency heists and revenue-generating IT schemes, have funded up to 50% of the country's missile projects. In November, the U.S. Treasury Department sanctioned eight North Korean agents linked to Kimsuky for their role in intelligence-gathering and revenue generation for Pyongyang's missile activities.

North Korea has dispatched thousands of tech-savvy workers to various countries, including China, Russia, Southeast Asia, and Africa, to infiltrate freelance networks and secure jobs that provide access to sensitive data and systems. These workers misrepresent themselves using falsified documents or purchased accounts to find remote jobs, often posing as citizens of other countries. Some of them use their privileged access to launch cyberattacks or exploit vulnerabilities in company systems. A recent indictment from the U.S. Department of Justice revealed that a group of individuals, including an Arizona woman, helped North Korean workers validate stolen identities and deceive U.S. companies, generating millions of dollars in wages and contributing to North Korea's evasion of U.S. sanctions.

North Korea's approach to cyber operations is distinct, treating its government as a criminal enterprise, with profits from illicit activities funneled directly into the regime. These schemes, which have included cryptojacking, targeting security researchers, and large-scale financial crimes, have helped fund the country's nuclear weapons program. North Korean IT workers, trained in science and mathematics, are closely monitored by the government and have limited freedom. Their operations involve building trust with companies and individuals over time, conducting reconnaissance, and maintaining long-term deception to continue siphoning funds and sensitive information for the regime's benefit.

The FBI has been investigating a North Korean scam that used fake companies employing real IT workers to funnel money back to the regime's military. The scam involved creating shell companies in the US, including Wyoming-based firms such as Culture Box LLC, Next Nets LLC, and Blackish Tech LLC, which posed as legitimate businesses offering freelance IT services. These companies hired virtual assistants and IT workers, often using false identities and American IP addresses, to perform legitimate contract work. Payments were funneled back to North Korea's Ministry of Defense and other agencies involved in weapons development. An American company, Registered Agents Inc., played a key role in filing the incorporation documents for these fake companies using fake personas. The Wyoming secretary of state has since revoked the business licenses of the implicated companies after receiving information from the FBI.

The FBI affidavit alleges that North Korean IT workers used domain names and LLCs registered in the US to mask their true identities and carry out fraudulent activities. These LLCs, sometimes created with the identities of individuals with previous ties to North Korean workers, were used to hire virtual assistants, recruit software developers, and receive payments for IT work. The Wyoming secretary of state's office has since increased audits of commercial registered agents and proposed legislation to prevent fraud and abuse of corporate filings, aiming to strengthen administrative authority to dissolve entities controlled by foreign adversaries.

Romance Scams from Nigeria

In this romance scam, Natasha Bridges, a fake identity created by a Nigerian scammer named Biggy, targeted men on Facebook by sending simple greetings, eventually tricking many into believing they had a romantic connection. Biggy, a "Yahoo boy," spent years pretending to be various personas, including that of Natasha, to con men out of money. The scam involved long-term manipulation, where Biggy would flirt and develop emotional connections with his victims before asking for money. Despite knowing it was a scam, many victims like James and Brett became emotionally invested, falling for Natasha's fabricated charm. The goal of these romance scams was to build trust and exploit vulnerability, all while Biggy played his role without remorse, seeing it as a stressful yet lucrative hustle.

This same kind of romance scam targeted Silvia, a successful Spanish dentist who believed she had found love with Brian, a divorced American soldier she met on Tinder. Despite her sons' skepticism, Silvia became deeply invested in the relationship, even buying rings for herself and Brian, and eagerly anticipating his arrival in Spain. However, her sons grew increasingly concerned when Brian claimed he had found bars of solid gold in a terrorist stash and needed her help to ship them. Recognizing the situation as a scam, her son Jaime warned his brother Carlos that they needed to intervene before their mother was further manipulated.

Online Fraud Network/Tech Spoofing in Europe

Law enforcement agencies from Germany, Albania, Bosnia-Herzegovina, Kosovo, and Lebanon have successfully shut down 12 locations linked to a criminal network responsible for thousands of daily scam calls. In mid-April 2024, police conducted searches at the suspects' residential and business premises, resulting in the arrest of 21 individuals and the seizure of data carriers, documents, cash, and assets totaling €1 million ($1.08 million). The network defrauded victims through various schemes, including fake police calls, investment fraud, and romance scams, with scammers posing as close relatives, bank employees, or police officers. Each country involved focused on different types of fraud, such as debt collection from Bosnia-Herzegovina and online banking fraud from Kosovo.

Investigators monitored the activities of the fraudsters in real-time, tracking up to 30 conversations simultaneously and linking the perpetrators' phone numbers to over 28,000 scam calls within just 48 hours. Europol reported that law enforcement efforts prevented financial losses for victims in over eighty percent of the cases investigated, with the potential damage from these scams estimated to exceed €10 million. The operation underscores the ongoing commitment of international law enforcement to combat organized crime and protect individuals from financial fraud.

In October 2019, Swiss authorities launched an investigation into a massive investment scam after receiving a complaint from a victim. The scam was linked to fraudulent call centers and websites of fake financial trading companies in Ukraine and later in Georgia. Though temporarily halted due to the war in Ukraine, the investigation resumed at the end of 2022, leading to coordinated actions in 23 countries. During these actions, various locations were searched, and suspects' bank accounts and assets were frozen. The scam involved over a hundred websites posing as legitimate investment companies offering cryptocurrency and trading options. Many victims, mainly Swiss and German, were lured into making substantial investments that were lost, with total losses amounting to at least several million euros.

Eurojust and Europol supported the complex cross-border investigation, with Eurojust helping to establish a joint investigation team between Swiss and Ukrainian authorities. Three coordination meetings were held to plan a coordinated action day, during which judicial measures were taken to freeze and seize the suspects' assets. Europol's European Financial and Economic Crime Centre and the European Cybercrime Centre assisted by providing analytical support and facilitating cooperation among the involved countries. Authorities from Switzerland, Germany, Belgium, Georgia, Ukraine, and several other European countries collaborated on a mutual legal assistance basis, leading to significant judicial measures across Europe.

Another growing form of fraud, known as spoofing or authorized push payment fraud, tricks consumers by impersonating trusted sources such as banks on messaging apps and requesting money transfers. Once the funds are sent, both the messenger and the money disappear. European policymakers are targeting this issue with new regulations, proposing that platforms like WhatsApp, Facebook, Amazon, and eBay could be held accountable for scams that originate on their services, similar to the liability faced by banks and payment service providers.

Online payment fraud is a global problem, with losses projected to reach $362 billion by 2028. However, approaches to combat this issue vary between the US and the European Union. While the US leans on technology like artificial intelligence to tackle fraud, the EU favors regulation. For example, the EU's Payment Services Regulation introduced mandatory double authentication for transactions, requiring two forms of ID verification. Although this reduced fraud, it led to complaints from online retailers, who saw a drop in sales as customers abandoned purchases during the additional verification process. In contrast, US retailers rely on automated fraud checks with comparable results to the EU's stricter regulations.

Spoofing fraud, where scammers impersonate legitimate entities like banks or government officials, is becoming increasingly common in the EU. To combat this, EU lawmakers are working on new regulations that would hold banks accountable for reimbursing customers who fall victim to such scams. The proposed rules, which extend beyond banks, would also target telecom operators and online platforms, requiring them to refund victims if they fail to remove fraudulent content. The measures aim to protect consumers from fake emails or calls impersonating public or private entities, building on the EU's existing Digital Services Act.

While the financial sector welcomes these changes, telecom operators are concerned about the potential financial and operational impact. Lobby groups warn that the new liability could cost up to €8 billion annually and may conflict with online privacy laws, as telecom providers would be expected to monitor phone calls in a similar way to social media content. Despite these concerns, proponents of the new regulations believe they could be a game-changer in addressing fraud, encouraging collaboration between banks and telecom operators to stop fake communications from legitimate-looking sources.

Why Stolen Funds Largely Cannot be Recovered?

Domestic vs. International Law Enforcement Jurisdiction

Last year, the FBI IC3 was only able to recover $538.39 million of the total $12.5 billion lost to online scams. In 2018, the FBI launched the IC3 Recovery Asset Team (RAT) to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

RAT only has jurisdiction over scammers operating inside America. In that respect, RAT recovered $538.39 million of the $758.05 million stolen domestically. The rest of the $12.5 billion was stolen by scammers living internationally.

The challenges of recovering stolen funds in cybercrimes often revolve around the complexities of domestic and international law enforcement jurisdictions. When a cybercrime transcends international borders, the situation becomes exponentially more complicated. While domestic efforts like RAT have seen some success, the broader picture reveals why recovering stolen funds remains such a significant challenge.

First, there’s a widespread lack of awareness among victims, which leads to underreporting of these crimes. Without proper reporting, the scale of the problem is underestimated, allowing scams to continue unchecked. Educating the public on how and why to report these incidents is crucial for tackling this issue head-on.

Secondly, the method through which the funds are stolen plays a critical role in determining their recoverability. For example, funds lost via gift cards or wire transfers are nearly impossible to trace, making recovery efforts futile.

Finally, the international nature of many scams creates a jurisdictional nightmare. Different countries have different legal frameworks and enforcement capabilities, and the lack of international cooperation often hampers recovery efforts. Victims must understand their local laws and report incidents appropriately to maximize any chance of recovery.

The Newest Technology Online Scammers Are Using in 2024

AI-Powered Scams and Emerging Threats

In the evolving landscape of cybercrime, AI-powered scams are becoming increasingly sophisticated and pervasive. Scammers are using advanced technologies to create highly convincing phishing emails and text messages, often impersonating trusted entities to steal sensitive information from unsuspecting victims. Deepfakes of celebrities are another alarming trend, where fabricated videos and images are used to promote fraudulent investment schemes, tricking people into parting with their money. Additionally, student loan forgiveness scams have become more prevalent, exploiting the financial vulnerabilities of students and graduates by promising relief in exchange for personal information or upfront fees (Global Guardian).

Phone scams and robocalls continue to be a major concern, with scammers using automated systems to reach a large number of potential victims. QR codes are also being exploited, with malicious codes leading to fraudulent websites designed to steal information or install malware. SIM swapping is another method where scammers take control of a victim’s phone number to intercept two-factor authentication codes and gain access to sensitive accounts. One-time-password (OTP) bots are used to automate this process, making it easier for scammers to bypass security measures. The variety and sophistication of these scams highlight the importance of staying vigilant and informed about the latest tactics being used by cybercriminals (Consumer FTC, World Economic Forum).

Emerging scams such as the "pig butchering" scam, where scammers build long-term relationships with victims to gain their trust and then steal their assets, are also gaining traction. This method, along with other region-specific scams, underscores the need for global cooperation and awareness to combat these threats effectively. By understanding the methods and tactics used by scammers, individuals can better protect themselves and contribute to the broader effort of reducing cybercrime globally.

Modern scams often utilize sophisticated technology to execute and mask their operations. Here's how:

Digital Identity Theft: A Growing Cyber Threat

Traditional identity theft often involves stealing personal information such as government ID numbers, credit card details, or biometric data to commit fraud. Similarly, digital identity theft allows cybercriminals to impersonate individuals within computer networks. However, it can be even more dangerous than traditional ID theft due to its complexity and reach.

Digital identities consist of software and algorithms that verify a person's or machine's identity online, such as persistent cookies that keep users logged into platforms like Google and Facebook or API keys. When these digital identities are stolen, malicious actors can gain unauthorized access, masquerading as legitimate users.

The rise of cloud services has significantly increased both the incentives for and risks associated with this type of cyber threat. Systems that rely on a single form of digital identity for verification are particularly vulnerable. According to Sandy Lau, district manager for Hong Kong and Macau at CyberArk, there's a risk that cookies could be stolen or exposed to third parties, who could then misuse them to access other applications or internal resources. The prevalence of hybrid work environments, where personal devices are used for work, further exacerbates this risk.

In response to these growing concerns, companies like CyberArk have developed solutions such as identity-centric secure browsers. Launched in March, this secure browser helps employees separate work-related and personal applications and domains, reducing the risk of cyber theft.

Large Language Models and Cybersecurity Risks

The launch of OpenAI's ChatGPT in late 2022 ignited a competition among tech companies to develop more advanced large language models (LLMs) with extensive datasets and sophisticated training methods. While these models offer many benefits, they have also become tools for cybercriminals, who use them to craft phishing messages or identify vulnerabilities in systems.

Hackers can leverage LLMs to automate the process of detecting weaknesses in targeted networks. Once access is gained, LLMs can be used to exploit these vulnerabilities further. According to a report by cybersecurity firm Palo Alto Networks, the median time between a system's initial compromise and data exfiltration dropped to just two days in 2022, a significant decrease from nine days in 2021.

Phishing attacks, which involve sending malicious links via email, text, or voice messages, remain a common method for infiltrating systems. However, LLMs have made these scams more convincing by generating more realistic messages on a larger scale. Fortunately, AI can also be a powerful tool for detecting fraudulent links and improving cybersecurity measures. For example, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) has been testing AI language models since May to detect phishing websites and enhance its risk alert system.

SuperSynthetic Identities

Generative AI has rapidly expanded into various areas, from generating vegan-friendly recipes to creating images of unlikely scenarios. However, not all uses of this technology are harmless. Fraudsters have harnessed AI to develop tools like WormGPT and FraudGPT, which enable more sophisticated and accessible cyberattacks. This rise in AI-driven fraud poses a significant threat to various industries, especially fintech companies that need to bolster their defenses against these evolving threats.

The progression of bots has led to the emergence of increasingly sophisticated forms, culminating in the development of SuperSynthetic™ identities. Unlike traditional synthetic identities that mix real and fake personal information, SuperSynthetic bots can deceive even the most advanced detection systems by mimicking legitimate customer behavior over time. This slow, calculated approach allows these bots to build trust with financial institutions, eventually leading to significant financial losses.

The threat posed by SuperSynthetics is unique in its patience and precision. These bots simulate real customer interactions over months, gradually gaining credibility before executing a final, lucrative fraud operation. Traditional fraud prevention methods, which rely on static data and individual identity verification, are no match for this new breed of bots. To effectively combat SuperSynthetic identities, financial institutions must adopt a more holistic approach that analyzes identities as part of a collective group or signature, rather than in isolation.

A shift in fraud prevention philosophy is essential for identifying and neutralizing SuperSynthetic bots. By adopting a big-picture perspective that considers digital footprints across a group of identities, banks can uncover patterns that individualistic tools might miss. This signature-based approach, combined with scalable real-time identity intelligence, offers a more robust defense against these advanced threats. As SuperSynthetic identities become more prevalent, it's imperative for financial institutions to adapt their strategies to protect their assets and customers.

Face Swapping Technology

Deepfake technology is increasingly being used by scammers, particularly a group known as the Yahoo Boys, to deceive victims in romance scams. These scammers, often based in Nigeria, use face-swapping software to create fake identities during video calls, making their fraudulent interactions appear more convincing. The technology allows them to change their appearance in real-time, which they use to build trust with their victims before tricking them into sending money. This new method of deception has been documented in numerous videos posted online by the scammers themselves, revealing the sophistication of their techniques.

Initially, the Yahoo Boys began using deepfakes in 2022 to send pre-recorded videos to potential victims, but they have since progressed to using real-time deepfake video calls. This shift has allowed them to engage more directly with their targets, making their scams more effective. These scammers operate through platforms like Zoom and use setups involving multiple phones or laptops to ensure the deepfakes are as convincing as possible. They often show their real faces alongside the fake personas, indicating a lack of fear regarding potential repercussions.

The Yahoo Boys are a loosely organized group with no clear leadership, operating in clusters that share tips and skills online. Their activities extend beyond romance scams to include business email compromises, cryptocurrency scams, and impersonation scams. They use social media and messaging platforms like Telegram to recruit members and advertise their scam techniques. Despite the decentralized nature of their operations, the group exhibits a high level of adaptability and sophistication, constantly evolving their methods to stay ahead of detection.

As deepfake technology improves, the potential for its misuse in scams is becoming a significant concern. The Yahoo Boys' use of deepfakes in romance scams is likely just the beginning, with the possibility of the technology being applied to other types of fraud. Experts like Rachel Tobac and Andrew Newell have noted the rapid advancements in face-swapping tools, making them more convincing and harder to detect. This trend suggests that scams involving deepfakes will become increasingly prevalent and challenging to combat.

Deep Live Cam

Recently, a software package called Deep-Live-Cam has gained significant attention on social media due to its ability to apply a person's face from a single photo to a live webcam video source. This software can track pose, lighting, and expressions in real time, making it easier than ever to deceive others remotely. Although the results aren't flawless, the rapid development of this technology shows how quickly the potential for remote deception is advancing. The software, which has been in development since late last year, became widely recognized after example videos featuring real-time deepfakes of public figures like Elon Musk and J.D. Vance went viral online. This attention briefly propelled the open-source project to the top of GitHub's trending repositories.

Deep-Live-Cam is not the first of its kind, but it represents a significant leap in the accessibility and usability of deepfake technology. Face-swapping technology, commonly known as deepfakes, originated in 2017 and was initially used in non-consensual pornography. At that time, the technology was expensive, slow, and did not function in real time. However, advancements in projects like Deep-Live-Cam have made it possible for anyone to use deepfake technology with just a regular PC and free software. The potential for misuse has also grown, as evidenced by past incidents, such as a $25 million heist in Hong Kong involving a deepfake video call. The increasing ease of creating real-time deepfakes poses a serious threat to individuals and organizations alike.

The Deep-Live-Cam software project, like many open-source GitHub projects, is a combination of several existing software packages integrated under a new interface. It relies on a pre-trained AI model called "inswapper" to perform the face swap and another model called GFPGAN to enhance the quality of the swapped faces by correcting artifacts and improving details. The inswapper model is particularly powerful because it was trained on a massive dataset of millions of facial images, allowing it to infer how a person's face might look from different angles, under varying lighting conditions, and with different expressions. This capability makes the face-swapping process more realistic and convincing.

Despite its current limitations, Deep-Live-Cam is part of a broader trend where face-swapping software is becoming more accessible and sophisticated. Other projects like facefusion offer similar capabilities, and as these technologies continue to develop, they will likely become easier to install and more effective. The potential for misuse, especially in fraud and deception, will grow as these tools improve and spread. As a result, it is crucial to remain vigilant about the ways such technology can be exploited and to consider the ethical implications of its use.

Victims’ Psychological and Emotional Damage

The rise of online scams has become an alarming trend, fueled by the increasing reliance on digital platforms for communication, commerce, and personal interactions. Cybercriminals have exploited this shift, creating sophisticated schemes that prey on people's trust and vulnerabilities.

As these scams grow more prevalent and complex, they not only result in financial losses but also leave victims grappling with significant psychological and emotional damage. The aftermath of such experiences can be devastating, leading victims to seek support and recovery options to rebuild their lives.

The impact of online scams extends beyond financial loss to significant psychological and emotional distress:

1. **Loss of Trust:** Victims often experience a deep sense of betrayal, which can lead to difficulty trusting others. This erosion of trust can extend beyond personal relationships, affecting professional interactions and general social engagement, making it challenging for victims to form new relationships or maintain existing ones.

2. **Stress and Anxiety:** The financial instability caused by scams can lead to prolonged stress and anxiety. This constant worry not only affects mental health but can also have physical health implications, such as increased blood pressure and other stress-related conditions.
3. **Depression:** The emotional toll of being scammed can lead to depression, especially if significant sums are lost or if there is public embarrassment. This depression can be debilitating, affecting the victim's ability to work, interact socially, and perform daily activities, further compounding their isolation and emotional distress.
4. **Shame and Isolation:** Victims might isolate themselves due to shame or fear of judgment from peers. This self-imposed isolation can prevent them from seeking the necessary help or support, exacerbating feelings of loneliness and making recovery even more challenging.

Seeking Support and Recovery

Recovering from an online scam involves more than recouping lost funds; it also requires addressing the psychological aftermath. Here are some steps victims can take:

1. **Report the Scam:** Contacting law enforcement and reporting to the Federal Trade Commission (FTC) or Internet Crime Complaint Center (IC3) can help authorities track and stop scammers.
2. **Seek Financial Advice:** Consulting with financial experts can help victims understand their options for financial recovery and prevent future incidents.
3. **Hire an Online Research Specialist:** Engaging an online research expert can help uncover essential online information, including financial or crypto transactions.
4. **Access Emotional Support:** Counseling or support groups for scam victims can be invaluable in helping to address feelings of betrayal and rebuilding trust.
5. **Educate Others:** Sharing experiences can empower other potential victims to recognize and avoid similar scams, turning a negative experience into a proactive tool for community awareness.

Where to go if you are an Online Scam Victim

If you fall victim to an online scam, here are some immediate steps you can take:

- **Local Law Enforcement:** Report to your local police, especially if the scam involves a significant amount of money. Involving law enforcement can also help document the incident, which may be crucial for insurance claims or tax deductions related to the loss.
- **Internet Crime Complaint Center (IC3):** File a complaint online with details of the scam. Providing detailed information can help law enforcement track down the perpetrators and potentially prevent others from falling victim to the same scam.
- **Federal Trade Commission (FTC):** Report the scam to the FTC, which handles consumer complaints and gathers data to prevent future fraud. The FTC also provides resources and guidance on how to recover from fraud and protect yourself from future scams.
- **Your Bank or Financial Institution:** Contact your bank or credit card company to discuss any transactions that need to be contested or security measures that should be put in place. Early intervention can prevent further unauthorized transactions and potentially reverse fraudulent charges.

International Resources

1. **Interpol - Online Scam Reporting:** Interpol provides resources and guidance on reporting cybercrime, including online scams, and works with national law enforcement agencies to address cross-border cyber threats.
2. **International Consumer Protection and Enforcement Network (ICPEN):** ICPEN offers resources for consumers to report scams and deceptive practices globally. They also provide information on consumer protection laws in various countries.
3. **Action Fraud (UK):** The UK's national fraud and cybercrime reporting center provides a platform for reporting scams and receiving advice on how to recover from online fraud.
4. **Canadian Anti-Fraud Centre (CAFC):** The CAFC offers support and information on reporting scams in Canada and provides resources for financial recovery and legal advice.
5. **Australian Cyber Security Centre (ACSC):** The ACSC offers a reporting platform for online scams and provides guidance on cybersecurity and scam recovery for individuals and businesses.
6. **NetSafe (New Zealand):** NetSafe provides a platform for reporting online scams and cyberbullying in New Zealand, offering support and advice on protecting yourself online.

Local Resources

1. **State Attorney General's Office (USA):** Many state attorney generals in the U.S. offer consumer protection services, including reporting online scams and seeking legal advice. Visit your state's Attorney General website for specific resources.
2. **State Consumer Protection Offices:** Many states have local consumer protection agencies that provide advice and resources for victims of online scams. These offices can assist with legal advice, mediation, and financial recovery.
3. **Community Legal Aid Services:** Local legal aid organizations often provide free or low-cost legal advice to victims of online scams. They can help you understand your rights and pursue legal action if necessary. Check your local directory or search online for legal aid services in your area.
4. **Local Law Enforcement:** Victims of online scams should also report the incident to their local police department. Many local law enforcement agencies have cybercrime units that specialize in investigating online fraud and can provide assistance and resources.

Emotional Support Resources

1. **Cybercrime Support Network (USA):** This network offers resources and support for victims of cybercrime, including emotional support and referrals to counseling services.
2. **Victim Support (UK):** Victim Support provides emotional and practical assistance to victims of crime, including those affected by online scams.
3. **Lifeline (Australia):** Lifeline offers crisis support and suicide prevention services, providing emotional support to those affected by online scams and other forms of cybercrime.
4. **Crisis Text Line (USA):** A free, 24/7 support service for individuals in crisis, including those impacted by online scams. Text HOME to 741741 to connect with a trained crisis counselor.

5 Tips to Avoid Online Scams in 2024

In today's digital age, the rise of online scams has reached alarming levels, with cybercriminals constantly devising new tactics to exploit unsuspecting victims. As these threats continue to grow, it is more important than ever to stay informed and vigilant. Understanding the evolving landscape of online scams and learning how to safeguard your personal information is crucial in protecting yourself from becoming a target.

Here are some strategies to better protect yourself from online scams in 2024.

1. **Use an Online Privacy Protection Tool:** An 24/7 active monitoring tool that scans the public data and dark web to alert you instantly if any of data is found online. Get alert of any potential threats via email or mobile app to take immediate action, securing your data and maintaining your privacy in today's digital world.
2. **Use a Password Manager:** Given the increasing number of accounts individuals manage, using a password manager can help generate and store complex, unique passwords for each account, reducing the risk of password reuse and improving security.
3. **Stay Informed About AI and Deepfake Technology**: Scammers are increasingly using AI and deepfake technology to create convincing scams, such as fake videos or audio recordings of trusted individuals. Stay informed about these technologies and be skeptical of unsolicited communications that seem too good to be true or suspicious in any way.
4. **Verify URLs and Email Addresses**: Before clicking on links or responding to emails, double-check the URL and email address for legitimacy. Scammers often use addresses that closely resemble legitimate ones, with slight variations.
5. **Use a VPN**: Using a Virtual Private Network (VPN) when accessing the internet, especially on public Wi-Fi, can help protect your data from being intercepted by malicious actors.
6. **Regularly Update Security Settings and Preferences**: Regularly review and update your security settings on social media, email accounts, and other online services to ensure you are taking advantage of the latest security features and privacy settings.

Conclusion

To combat these technological challenges, individuals and organizations need to stay vigilant, enhance their cybersecurity practices, and employ advanced security measures to protect themselves from scams. Regularly updating software, using strong and unique passwords, implementing multi-factor authentication, and being cautious of unsolicited communication can all contribute to minimizing the risks associated with scams. Additionally, staying informed about the latest scam tactics and maintaining a healthy skepticism towards suspicious requests or offers can go a long way in safeguarding against the technology-driven landscape of scams.

By staying informed and adopting proactive measures, you can shield yourself from falling victim to these scams. Be skeptical of unsolicited contacts, enable multifactor authentication, and conduct thorough research before making purchases or donations. If you encounter suspicious activity or become a victim of a scam, report it to the relevant authorities promptly.

Remember, protecting your identity is an ongoing process. Regularly monitor your credit report, consider enrolling in credit monitoring services, and take advantage of identity theft insurance for added peace of mind. By staying vigilant and informed, you can safeguard yourself against the ever-evolving threats posed by scammers in 2024 and beyond.