Third Annual Study: State of Internet Scams 2023

Table of Contents

Introduction

A record $10.3 billion was lost by Americans to online scams in 2022, up from $6.9 billion in 2021, and up 277% from $2.7 billion five years ago, according to the FBI Internet Crime Complaint Center. The average loss per victim jumped from $8,142 per incident in 2021 to $12,859 last year.

The most alarming part, however, is a new survey of 5,500 online scam victims that found that most of the victims suffered from romance scams.

Victims of online scams – whether it be investment, romance, cryptocurrency or others – often lose their life savings and some even take their own lives. In our analysis we found that only 4.2% of lost monetary assets were recovered in 2022.

Social Catfish is releasing its third annual study on the State of Internet Scams 2023.

The purpose of this 33 page study is to offer a comprehensive and real time overview to equip people with the knowledge required to avoid becoming a victim.

The mission of Social Catfish is to help eradicate online scams using reverse search technology.

Methodology

- We analyzed data released in 2023 by the FBI Internet Crime Complaint Center (IC3) and the Federal Trade Commission (FTC).
- We released proprietary survey results after polling 5,500 online scam victims. The respondents are members of the Social Catfish Facebook group SCF Seekers – a place for victims who have been scammed out of money.

10 Key Findings

1. **Total Reported Money Lost**: A record $10.3 billion was lost to online scams in 2022, up from $6.9 billion in 2021. The average loss per victim was $12,859 in 2022, up from $8,142 the previous year.
2. **81% of Romance Scam Victims Do Not Come Forward:** 4,455 of 5,500 victims polled by Social Catfish said they were too ashamed to come forward and file a formal report with the FBI or FTC.
3. **$200 Billion Estimated Actual Losses in 2022:** Given many online scam victims are too afraid to come forward, we estimate actual losses were closer to $200 billion in 2022.
4. **Only 4.2% of Stolen Funds Were Recovered:** The FBI IC3 Recovery Asset Team was only able to recover $433 million, or 4.2%, of the total $10.3 billion lost in 2022. The primary reason is most scams originate from outside the U.S. where law enforcement has no jurisdiction.
5. **Teens & Children See Largest % Increase in Money Lost:** From 2021 to 2022 victims under 20 saw a 107% increase in money lost, the largest among all age groups, including seniors. Seniors still have the highest total losses at $3.1 billion lost
6. **Apps Where Most People are Scammed**: The Social Catfish poll of 5,500 online scam victims found most online scams happen on Facebook with 32%, Google Hangouts with 16%, WhatsApp with 16%, Instagram with 14%, and Plenty of Fish with 16%.
7. **The Future of Online Scams has Arrived With Artificial Intelligence**: The explosion of AI has given us a glimpse into the future of scams with new tactics such as **'voice cloning' and 'deepfake' videos** making it look and sound like you are giving money to someone you know, trust or love.
8. **10 States with the Most Online Scams:** California, Florida, Texas, New York, New Jersey, Washington, Illinois, Virginia, Arizona, and Pennsylvania.
9. **Top 20 Most Scammed Countries, U.S. is No. 1:** The United States led the world with 466,501 online scam victims in 2022. The United Kingdom, Canada, India, and Australia round out the top five.
10. **5 Costliest Scams in the U.S. from 2020 - 2022:** BEC, Investment, Romance, Personal Data Breach, and Tech Support.

Examples of the Costliest Scams in 2023 and How to Avoid Them

3 Most Common Investment Scams

Investment scams are designed to deceive people and steal their money by promising high returns or exclusive investment opportunities. While there are various types of investment scams, here are three common ones and some tips on how to avoid falling victim to them:

1. **Ponzi Schemes:** Promises of high, guaranteed returns with little or no risk.

   Tips to Avoid: Be skeptical of unrealistic returns and always research the investment opportunity thoroughly. Ask for verifiable proof of past returns and check the legitimacy of the company and its founders.

2. **Fake Investment Clubs:** Scammers pose as investment clubs or groups and promise pooled funds for investments.

   Tips to Avoid: Verify the legitimacy of investment clubs by checking their registration with appropriate authorities and seeking advice from trusted sources.

3. **Real Estate Investment Scams:** Fraudulent real estate investment opportunities that promise high returns but don't deliver.

   Tips to Avoid: Verify property ownership and legitimacy, and conduct due diligence on real estate investment opportunities. If it sounds too good to be true, it probably is.

3 Most Common Crypto Scams

The unprecedented rise in investment scams in 2022 was largely due to crypto-investment scams which stole a record $2.57 billion last year.

1. **Fake ICOs (Initial Coin Offerings):** Scammers create fraudulent ICOs to capitalize on the hype around new cryptocurrencies.

   Tips to Avoid: Conduct thorough research on the project team, the technology, and the use case. Look for legitimate projects with transparent whitepapers and active communities.

2. **Fake Exchanges and Wallets:** Scammers set up fake exchanges or wallet services to steal users' funds.

   Tips to Avoid: Only use reputable and well-known exchanges and wallets. Verify the website's URL and look for security measures like 2FA and cold storage for funds.

3. **Pump and Dump Schemes:** Scammers artificially inflate the price of a low-cap cryptocurrency by spreading false information, then sell their holdings at the peak, causing a price crash.

   Tips to Avoid: Be cautious of sudden price spikes based on unsubstantiated claims, and research before investing in lesser-known tokens.

3 Most Common BEC Scams

Business Email Compromise (BEC) scams, also known as CEO fraud or email impersonation scams, target businesses and organizations. These scams typically involve fraudulent emails that deceive employees into taking actions that benefit the scammers financially. Here are three common types of BEC scams and tips on how to avoid falling victim to them:

1. **Invoice Fraud:** In this type of BEC scam, scammers send emails posing as a legitimate vendor or supplier. They provide altered payment instructions, such as a different bank account, and request that the payment be made accordingly. If the employee falls for the scam, the payment is sent to the scammer's account, resulting in financial loss for the organization.

   Tips to Avoid:

   - Implement a robust verification process for any changes to payment instructions, such as contacting the vendor directly through a verified contact number.
   - Educate employees about the risks of invoice fraud and the importance of independently verifying payment instructions.
   - Be cautious of unexpected or urgent requests to change payment details and double-check the legitimacy of such requests.

2. **Executive Impersonation:** In this scam, scammers impersonate high-ranking executives within the organization, such as the CEO or CFO, and send emails to

employees in finance or accounting departments. The emails typically request urgent wire transfers or the disclosure of sensitive financial information.

Tips to Avoid:

- Establish a clear protocol for approving and verifying financial transactions, including multi-factor authentication and confirmation from multiple parties.
- Encourage employees to verify any unusual or urgent requests through an alternative communication channel, such as a phone call or in-person conversation.
- Train employees to recognize warning signs of executive impersonation, such as slight variations in email addresses or unusual email behavior.

3. **Employee Payroll Diversion:** In this BEC scam, scammers gain access to employee payroll information and redirect direct deposit payments to their own accounts. They may accomplish this by using phishing techniques or compromising internal systems.

   Tips to Avoid:

   - Implement robust cybersecurity measures, such as employee training on phishing awareness, multi-factor authentication, and regular system updates.
   - Regularly review and monitor access controls and privileges within the organization's systems.
   - Encourage employees to report any suspicious emails, especially those requesting changes to payroll information.

3 Most Common Tech Support Scams

Tech support scams are fraudulent activities where scammers pose as technical support representatives to deceive individuals into providing sensitive information, granting remote access to their computers, or paying for unnecessary services. Here are three common types of tech support scams and tips on how to avoid them:

1. **Phone Call Scams:** In this type of scam, fraudsters make unsolicited phone calls, claiming to be from well-known technology companies or computer support

providers. They may inform the victim of a supposed issue with their computer or software and try to convince them to provide remote access or disclose personal and financial information.

Tips to Avoid:

- Be cautious of unsolicited calls claiming to be from tech support. Legitimate companies generally do not proactively reach out to customers in this manner.
- Do not provide personal information or grant remote access to your computer unless you have independently verified the legitimacy of the caller.
- Hang up if you suspect a scam and report the incident to the appropriate authorities.

2. **Pop-up Scams:** In this scam, fake pop-up windows or error messages appear on the victim's computer screen, claiming that their device is infected with malware or experiencing technical issues. The pop-ups often provide a phone number or website to call for assistance, connecting the victim with scammers who impersonate tech support.

   Tips to Avoid:

   - Do not click on suspicious pop-ups or error messages, especially those that prompt you to call a specific number for support.
   - Install reputable antivirus or anti-malware software and keep it up to date to help detect and prevent malicious pop-ups.
   - If a pop-up appears, close your browser or use task manager to terminate the browser process if necessary.

3. **Online Ads or Search Engine Scams:** Scammers create deceptive online advertisements or manipulate search engine results to appear at the top of search results for tech support-related queries. These ads or search results often lead users to fraudulent websites that mimic legitimate tech support providers.

   Tips to Avoid:

- Be cautious when clicking on online ads or search results, especially if they appear overly promotional or too good to be true.
- Verify the legitimacy of tech support providers by independently researching their website, contact information, and customer reviews.
- Do not provide personal or financial information on unfamiliar websites and avoid downloading software from untrusted sources.

3 Most Common Personal Data Breach Scams

Personal data breach scams involve the unauthorized access, theft, or misuse of personal information for fraudulent purposes. Here are three common types of personal data breach scams and tips on how to avoid them:

1. **Phishing Scams:** Phishing scams are prevalent and typically involve fraudulent emails, text messages, or websites that impersonate legitimate organizations or individuals. The goal is to trick recipients into revealing their personal information, such as login credentials or financial details.

   Tips to Avoid:

   - Be cautious of unsolicited messages or emails asking for personal information. Legitimate organizations usually do not request sensitive data via email.
   - Check the sender's email address, as scammers may use deceptive or slightly altered addresses to mimic legitimate sources.
   - Avoid clicking on links or downloading attachments from suspicious emails or messages.
   - Verify the legitimacy of requests by contacting the organization directly through their official website or phone number.

2. **Data Breach Notification Scams:** Scammers exploit data breaches to target individuals by sending fraudulent emails or messages claiming that their personal information was compromised. They may provide a link or attachment that leads to further data theft or malware installation.

   Tips to Avoid:

- Independently verify the legitimacy of data breach notifications by visiting the official website of the organization or contacting their customer support directly.
- Be cautious of unsolicited notifications that require immediate action or ask for sensitive information.
- Avoid clicking on links or downloading attachments from suspicious emails or messages related to data breaches.
- Regularly monitor your financial accounts and credit reports to detect any unauthorized activity.

3. **Social Engineering Scams:** Social engineering scams involve manipulating individuals into disclosing personal information or performing actions that benefit scammers. This can occur through phone calls, emails, or even in-person interactions.

   Tips to Avoid:

   - Be skeptical of requests for personal information, especially if they come from unfamiliar sources or seem unusual or unexpected.
   - Do not provide personal information over the phone or email unless you have independently verified the legitimacy of the request.
   - Be cautious of individuals or organizations that pressure you to act quickly or create a sense of urgency.
   - If in doubt, verify the legitimacy of the request or interaction by contacting the organization directly through trusted contact information.

3 Most Common Romance Scams

Romance scams are a prevalent form of online fraud that targets individuals seeking love, companionship, or romantic relationships. According to the poll we conducted on Facebook to 5,500 followers, most people fell victim to this type of scam because of emotional vulnerability. Romance scams were also chosen by our followers as the most common scam suffered. Here are three common types of romance scams and some tips on how to avoid falling victim to them:

1. **Catfishing Scams:** In this type of scam, fraudsters create fake profiles on dating websites or social media platforms to establish a romantic connection with their victims. They often use stolen photos and invent elaborate stories to gain the

victim's trust. Eventually, they may request money for various reasons, such as medical emergencies or travel expenses.

Tips to Avoid:

- Perform a reverse search to confirm the identity of the individual you are talking to online.
- Be cautious of individuals who refuse to meet in person or engage in video calls.
- Use reverse image search tools to verify the authenticity of profile pictures.
- Be wary of individuals who profess their love or ask for financial assistance too quickly in the relationship.
- Don't send money or provide financial information to someone you've only met online.

2. **Military Romance Scams:** Scammers may impersonate military personnel deployed overseas and exploit the trust and admiration associated with those serving in the military. They create emotional connections and then request money for supposed emergencies, such as medical bills or travel expenses.

   Tips to Avoid:

   - Verify the identity of individuals claiming to be in the military by requesting official documentation or contacting their military base directly.
   - Be skeptical if they avoid video calls or make excuses for not meeting in person.
   - Research common military scams and familiarize yourself with warning signs and red flags.
   - Be cautious of requests for financial assistance, especially if they are accompanied by emotional manipulation.

3. **Investment Scams:** In investment romance scams, fraudsters pose as wealthy individuals or entrepreneurs looking for romantic partners. They entice victims with promises of lucrative investment opportunities or joint business ventures. Once the victim is emotionally invested, the scammer requests money for investments that do not exist.

Tips to Avoid:

- Be wary of individuals who present themselves as wealthy or successful entrepreneurs without verifiable proof.
- Conduct thorough research on any investment opportunity before committing funds.
- Consult a trusted financial advisor or conduct due diligence to verify the legitimacy of investment proposals.
- Avoid sharing financial information or making financial transactions with someone you've only met online.

The Future of Online Scams: Artificial Intelligence

Artificial intelligence (AI) has the potential to significantly impact the landscape of online scams, enabling scammers to create more sophisticated and convincing schemes.

7 Types of AI Deepfake Video Scams

The use of AI deepfake videos and voice cloning in online scams is a growing concern. Scammers are leveraging these technologies to manipulate and deceive individuals for fraudulent purposes.

1. **Impersonation Scams:** Scammers can use AI deepfake technology to create videos or audio recordings that mimic the voices and appearances of trusted individuals, such as family members, friends, or authority figures. They may impersonate someone close to the victim and request financial assistance or sensitive information, leading to financial loss or identity theft.
2. **CEO Fraud and Business Scams:** AI deepfake videos or voice cloning can be used to impersonate high-ranking executives within organizations. Scammers can manipulate videos or audio recordings to mimic the CEO's voice and appearance, then use these to deceive employees into making unauthorized financial transactions or sharing confidential company information.
3. **Romance Scams:** In romance scams, scammers create fake personas and develop relationships with unsuspecting individuals online. AI deepfake videos or voice cloning can be employed to simulate video calls or voice conversations, making the scam appear more authentic and convincing. The scammers can

further manipulate the multimedia content to deceive victims emotionally and financially.

4. **Face Swapping:** Deepfake technology can be used to swap the faces of individuals in videos, making it appear as if someone else is speaking or acting. For example, there have been deepfake videos that replace the faces of celebrities with other famous individuals, creating the illusion that they are performing in a movie or TV show.

5. **Political Figures:** Deepfake videos have been created featuring politicians, altering their speeches or actions to spread false information or generate controversy. Such videos have the potential to disrupt political campaigns or manipulate public opinion.

6. **Revenge Porn:** Deepfake videos have been a cause for concern in the context of revenge porn, where someone's face is superimposed onto explicit content without their consent. This has serious implications for privacy, consent, and the potential harm it can cause to individuals involved.

7. **Historical Figures:** Deepfake videos have been created using historical footage, manipulating the actions or speeches of notable figures from the past. While these videos can be entertaining or educational when used responsibly, they also raise concerns about historical accuracy and the potential for misinformation.

How to Avoid AI Deep Fake and AI Voice Cloning Scams

- **Be cautious of unsolicited requests:** If you receive a phone call or message from someone requesting personal information or financial transactions, be skeptical, especially if it seems out of the ordinary. Verify the identity of the person through other means before sharing sensitive information.

- **Secure your personal information:** Be mindful of the information you share online, especially on social media platforms. Limit the amount of personal information publicly available, as scammers can use it to create more convincing scams.

- **Enable two-factor authentication (2FA):** Enable 2FA for your online accounts whenever possible. This adds an extra layer of security by requiring a secondary verification method, such as a unique code sent to your phone, in addition to your password.

- **Stay informed about AI scams:** Stay updated on the latest AI scam techniques and trends. Awareness can help you identify potential scams and avoid falling

victim to them. Follow reliable news sources and organizations that specialize in cybersecurity for the latest information.

- **Verify the source of information:** If you come across a video or audio clip that seems suspicious or too good to be true, take the time to verify its authenticity. Cross-reference the information with trusted sources or contact the individual or organization directly to confirm its legitimacy.
- **Be critical of media content:** Develop a critical eye when consuming media content, especially online. Look for signs of manipulation, such as unnatural facial movements, mismatched audio and video, or inconsistencies in the content. Use reputable fact-checking sources to verify the accuracy of information.
- **Report suspicious activity:** If you encounter a suspected voice cloning or deep fake scam, report it to the relevant authorities, such as law enforcement agencies, online platforms, or cybersecurity organizations. By reporting scams, you can help prevent others from becoming victims.

Other potential ways AI could shape the future of online scams:

1. **Advanced Phishing Attacks:** AI-powered phishing attacks could become more convincing and difficult to detect. Scammers could leverage AI algorithms to craft highly personalized and targeted phishing emails that mimic the communication style and patterns of the victim's contacts, making them more likely to fall for the scam.
2. **Voice and Video Manipulation:** Deepfake technology, driven by AI, could be employed to create realistic audio and video impersonations. Scammers could use this technology to imitate the voices of individuals in authority or create fraudulent video messages, making it harder for victims to discern the authenticity of the content.
3. **Chatbot Scams:** AI-powered chatbots can engage in realistic and automated conversations with users. Scammers could use chatbots to pose as customer service representatives, collecting sensitive information or convincing users to disclose personal details or financial credentials.
4. **Social Engineering Attacks:** AI can be utilized to analyze large amounts of data from social media platforms and other online sources, allowing scammers to gather extensive information about their targets. This data can then be used to create personalized social engineering attacks, increasing the chances of successful manipulation.

5. **Malware and Cyber Attacks:** AI can enhance the capabilities of malware and cyberattacks. AI algorithms can be employed to develop malware that can adapt and evolve, making it more challenging for traditional security measures to detect and mitigate these threats effectively.
6. **Fake News and Disinformation:** AI algorithms can generate highly convincing fake news articles, blogs, or social media posts. Scammers may exploit this technology to spread disinformation, manipulate public opinion, or launch misinformation campaigns for political or financial gain.
7. **Fraud Detection Evasion:** On the flip side, scammers can also employ AI to bypass fraud detection systems. By studying and understanding the techniques used by anti-fraud systems, scammers can develop strategies to evade detection and improve the success rate of their fraudulent activities.

Misinformation and Societal Impacts

Deep fake videos raise concerns about misinformation and the erosion of trust in visual media. Malicious actors can spread false information, create fabricated evidence, or damage the reputation of individuals or organizations. Deep fakes also have the potential to exacerbate the spread of misinformation in an already complex and interconnected digital landscape. They can have significant societal impacts, including the potential to influence elections, incite social unrest, or undermine public figures and institutions.

Why Stolen Funds Largely Cannot be Recovered: Domestic vs. International Law Enforcement Jurisdiction

Last year, the FBI IC3 was only able to recover $433 million of the total $10.3 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 $433 million of the $590 million stolen domestically.

The rest of the $10.3 billion was stolen by scammers living internationally. The majority of online scams emanate from Nigeria where scamming is a full blown business sector in a country where many citizens lack financial opportunity.

Reasons Recovering funds is challenging for banks and governments:

1. **Jurisdictional issues:** Online scammers can operate from anywhere in the world, making it difficult to determine their actual location and hold them accountable. They often hide behind anonymous identities or use techniques like IP spoofing to obfuscate their true origins. This jurisdictional complexity makes it hard for authorities to pursue legal action and recover funds.
2. **Encryption and anonymization:** Scammers often use encryption and anonymization tools to conceal their activities and protect their identities. This makes it challenging for law enforcement agencies and financial institutions to trace transactions and identify the individuals behind the scams.
3. **International cooperation:** Coordinating efforts among different countries and their respective law enforcement agencies can be complex and time-consuming. It requires cooperation and information sharing between jurisdictions, which may face legal, bureaucratic, or logistical challenges.
4. **Rapid movement of funds:** Scammers are adept at swiftly moving funds through various accounts and financial channels, making it difficult to trace and freeze the money before it is withdrawn or transferred to other jurisdictions.
5. **Lack of victim reporting:** Not all victims of online scams report their losses to banks or authorities. Some may feel embarrassed, blame themselves, or believe that reporting won't make a difference. Without sufficient reporting, it becomes harder to gather comprehensive data and take appropriate actions.
6. **Limited resources:** Banks and government agencies have limited resources and priorities. Investigating and recovering funds lost to online scams often requires significant resources, including specialized cybercrime units, trained personnel, and advanced technologies. Allocating these resources can be challenging due to competing priorities.

While recovering funds lost to online scams can be difficult, banks and governments have taken steps to improve security measures, educate the public about scams, and enhance cooperation between different stakeholders. However, prevention, awareness, and personal diligence remain crucial in avoiding online scams and protecting oneself from financial losses.

Global Reach of Online Scams

Where Do Online Scams Originate From?

Online scams can originate from various parts of the world, and it's challenging to pinpoint a specific geographical location as the sole source of most scams. Scammers can operate from any country and target victims globally due to the nature of the internet and its borderless nature. However, certain regions have been known to have a higher concentration of online scam activities. These regions include:

1. **West Africa, particularly Nigeria:** Nigeria has gained notoriety for being associated with various types of online scams, most notable romance scams.
2. **Eastern Europe, including Russia and Ukraine:** This region has been associated with cybercriminal activities, including the development and distribution of malware, hacking, and financial frauds such as phishing and identity theft. Romania and Bulgaria have also been linked to various forms of online scams, including phishing, card skimming, and online auction fraud.
3. **Southeast Asia:** Countries in Southeast Asia, such as the Philippines, Indonesia, and Malaysia, have seen an increase in online scams. Some of the common scams originating from this region include online romance scams, job scams, and lottery scams.

It's important to note that these regions should not be seen as the exclusive sources of online scams. Scammers can operate from anywhere in the world, and their tactics and techniques continue to evolve. It's crucial for individuals to remain vigilant and practice online security measures regardless of the origin of the scams.

These are the 20 Most Scammed Countries

The United States is the No. 1 most scammed country in the world with 466,501 victims in 2022. The United Kingdom, Canada, India, and Australia round out the top five.

Why are America and Other Developed Nations Targeted the Most?

1. **Economic Factors**: Countries with strong economies and high levels of financial activity may attract scammers who seek to exploit potential victims for monetary gain. Scammers often target regions where people have disposable income and financial resources.
2. **Technological Advancements**: Countries with advanced technological infrastructure and widespread internet access give scammers more opportunities to exploit and penetrate sophisticated online systems.

3. **Global Connectivity**: Countries that have significant international connections, including trade and travel, are more susceptible to online scams. Scammers will have more opportunities to target individuals from different countries. The countries you mentioned are major players in global trade and have extensive connections with other nations, making them potential targets for scams.
4. **Popularity and Awareness**: It's also worth noting that the inclusion of specific countries on these lists could be influenced by the level of awareness and reporting of scams in those regions. Countries with higher levels of awareness and reporting mechanisms may have more documented cases of scams, leading to a perception that scams frequently originate from those locations.

Online Scams by Age Group

5 online scams targeting children and teens

Online scams targeting children and teens can be particularly concerning as they exploit their innocence, lack of experience, and trust. Here are five common online scams that specifically target children and teenagers:

1. **Online Identity Theft:** Scammers may create fake social media accounts or gaming profiles to impersonate peers or influencers that children admire. They use these fake identities to manipulate children into sharing personal information, such as passwords, addresses, or financial details. This information can be used for identity theft, cyberbullying, or other fraudulent activities.
2. **Fake Online Contests and Giveaways:** Scammers create fake contests or giveaways on social media platforms or websites that target children and teenagers. They entice them with promises of winning popular gadgets, merchandise, or virtual currency in exchange for personal information or small payments. However, these contests are scams, and the scammers disappear once they obtain the requested information or money.
3. **In-App Purchases and Unauthorized Charges:** Many mobile games and apps offer in-app purchases, where users can buy virtual items or currency. Scammers take advantage of this by tricking children into making unauthorized purchases or subscribing to costly services without parental consent. They often use deceptive tactics to lure children into these transactions, resulting in unexpected charges for their parents or guardians.

4. **Phishing Scams and Fake Websites:** Children and teenagers may receive fraudulent emails, messages, or links that appear to come from trusted sources, such as gaming platforms or social media networks. These scams aim to trick them into revealing login credentials, personal information, or credit card details. Scammers may create fake websites that mimic popular gaming or entertainment platforms to deceive young users.

5. **Online Predators and Grooming:** This scam involves individuals posing as friends or potential romantic interests to establish relationships with children and teenagers. They gain their trust over time through online platforms, chat rooms, or social media. The scammers exploit these relationships to manipulate, exploit, or engage in inappropriate activities, such as sextortion or solicitation of explicit content.

   How to Avoid

   - Educate children and teenagers about online scams, emphasizing the importance of privacy, not sharing personal information, and verifying the authenticity of online requests.
   - Encourage open communication and maintain a trusting relationship, so children feel comfortable discussing their online activities and interactions.
   - Implement parental controls and monitor online activities to prevent unauthorized purchases or interactions with strangers.
   - Teach children about responsible internet usage, including avoiding suspicious links, not engaging with unknown individuals, and reporting any concerning or inappropriate behavior.
   - Use reputable antivirus and internet security software to protect devices from malware and phishing attempts.
   - Stay informed about popular online platforms, games, and social media trends to understand the potential risks and scams associated with them.

5 Online Scams Targeting Seniors

Seniors are often targeted by scammers due to various reasons, including their perceived vulnerability, potentially higher savings, and limited knowledge of emerging online threats. Here are five common online scams that specifically target seniors:

1. **Medicare/Healthcare Scams:** Scammers pose as representatives from healthcare agencies, insurance companies, or Medicare providers to exploit seniors' concerns about their health coverage. They may offer fake services, discounts, or products, aiming to obtain personal information, Medicare numbers, or financial details.

2. **Investment and Financial Scams:** Scammers target seniors with fraudulent investment opportunities, promising high returns or exclusive deals. They may use convincing websites, emails, or phone calls to manipulate seniors into investing in non-existent businesses, Ponzi schemes, or get-rich-quick schemes. Seniors can suffer significant financial losses as a result.

3. **Tech Support Scams:** Scammers contact seniors via phone calls or pop-up messages on their computers, pretending to be tech support representatives from well-known companies. They claim that the senior's device has a virus or technical issue and offer to fix it remotely for a fee. In reality, they gain access to personal information or install malicious software on the senior's device.

4. **Sweepstakes/Lottery Scams:** Seniors are often targeted with fraudulent sweepstakes or lottery schemes, where scammers inform them that they have won a large sum of money or a valuable prize. However, to claim the prize, they must pay upfront fees or provide personal information. The promised winnings do not exist, and seniors end up losing money or falling victim to identity theft.

5. **Romance Scams:** Scammers create fake online dating profiles and build relationships with seniors, gaining their trust and emotional investment. They may create elaborate stories or feign affection to manipulate seniors into sending money, gifts, or providing financial support. Once the scammers have obtained what they want, they disappear, leaving the senior emotionally and financially devastated.

How to Avoid

- Educate seniors about common online scams and the tactics scammers use to manipulate them.
- Encourage seniors to be skeptical of unsolicited phone calls, emails, or online messages, especially those requesting personal information or money.
- Advise seniors to consult trusted family members or friends before making financial decisions or sharing sensitive information.

- Remind seniors to keep their computer systems and antivirus software up to date to protect against malware and phishing attempts.
- Encourage seniors to regularly review their financial statements, credit reports, and Medicare statements for any suspicious activities.
- Promote a supportive and open environment where seniors feel comfortable discussing their concerns, experiences, and potential scams

Online Scams Targeting Minority Groups

While scammers can target individuals of any race or ethnicity, certain scams may exploit specific vulnerabilities or cultural factors.

5 online scams that can disproportionately target Black Americans:

1. **Employment and Job Scams:** Scammers may post fake job listings or work-from-home opportunities specifically targeting Black Americans seeking employment. They may claim to offer high-paying jobs or career advancement opportunities, but in reality, they aim to collect personal information, engage in identity theft, or request upfront payments for fake training or background checks.
2. **Grant and Financial Aid Scams:** Scammers target individuals seeking financial assistance for education, small businesses, or community projects. They may pose as government officials or representatives of grant programs specifically designed for minority communities. These scammers ask for upfront fees or personal information, promising access to grants or financial aid that never materializes.
3. **Housing and Rental Scams:** Black Americans looking for housing or rental opportunities can be targeted by scammers who post fake listings or engage in discriminatory practices. They may request payment for security deposits or application fees for properties that do not exist or are not available for rent. In some cases, scammers may exploit housing discrimination by promising exclusive listings or favorable terms.
4. **Dating and Romance Scams:** Scammers create fake profiles on dating websites or social media platforms, targeting Black Americans seeking companionship or romantic relationships. They build emotional connections, often using stolen photos or false identities, to manipulate victims into sending

money or providing financial assistance for various reasons, such as medical emergencies or travel expenses.

5. **Charity and Donation Scams:** During times of crisis or in response to community needs, scammers may set up fake charity organizations or crowdfunding campaigns that specifically appeal to Black Americans. They exploit the desire to support causes related to racial justice, community empowerment, or social equality, but divert the funds for personal gain without actually fulfilling the intended purpose.

   How to Avoid

   - Stay vigilant and be cautious of unsolicited offers, requests for personal information, or upfront payments.
   - Research and verify the legitimacy of job opportunities, grant programs, rental listings, or charitable organizations before providing any personal information or making financial commitments.
   - Be skeptical of online relationships and avoid sending money to individuals met online, especially if there are red flags or inconsistencies in their stories.
   - Report scams or suspicious activities to local law enforcement, relevant online platforms, and consumer protection agencies.
   - Stay informed about common scam tactics and share information within the community to raise awareness and prevent others from falling victim to similar scams.

It is essential to empower and educate the Black community about these scams, promote financial literacy, and foster a supportive environment where individuals can seek guidance and report fraudulent activities.

5 online scams that can disproportionately target Hispanic Americans:

1. **Immigration and Citizenship Scams:** Scammers may target Hispanic Americans who are seeking information or assistance with immigration or citizenship processes. They may pose as immigration attorneys, consultants, or government officials, promising faster or guaranteed results in exchange for upfront fees or personal information. These scams can exploit the anxieties and aspirations related to immigration status.

2. **Employment Scams:** Hispanic Americans seeking employment opportunities may be targeted by scammers who post fake job listings or offer work-from-home opportunities. These scams may exploit language barriers, cultural factors, or the desire for stable employment. Scammers may request payment for training materials, background checks, or job placements that never materialize.

3. **Notario Fraud:** Notarios, or notaries, hold different roles and responsibilities in the United States compared to Latin American countries. Scammers may take advantage of this confusion and pose as notarios offering legal services, including immigration assistance or document translations. They exploit the trust associated with notarios in Latin American communities and may provide inaccurate or fraudulent services.

4. **Lottery and Sweepstakes Scams:** Hispanic Americans can be targeted by scams involving fake lottery winnings or sweepstakes prizes. Scammers may claim that the victim has won a large sum of money or a valuable prize but must pay taxes, fees, or provide personal information to claim the winnings. In reality, the prizes do not exist, and the victims end up losing money or falling victim to identity theft.

5. **Family Emergency Scams:** Scammers may exploit the close-knit nature of Hispanic families by impersonating a family member in distress. They contact individuals, usually older family members, claiming to be a relative facing an urgent situation or in need of financial assistance. These scams play on emotions and the desire to help family members, leading victims to send money or disclose personal information.

   How to Avoid

   - Be cautious of unsolicited communications, especially those requesting personal information, financial details, or upfront payments.
   - Seek reliable and trustworthy sources of information and services, such as government agencies, reputable legal professionals, or recognized organizations specializing in immigration matters.
   - Educate yourself and others about common scam tactics and red flags to be aware of.
   - Verify the legitimacy of job opportunities, lottery winnings, or requests for financial assistance before providing any personal information or making financial commitments.

- Encourage open communication within the community to share experiences and warn others about potential scams.
- Report scams to local law enforcement, relevant government agencies, and consumer protection organizations to help protect others and raise awareness.

5 online scams that can disproportionately target Asian Americans:

1. **Tech Support Scams:** Scammers may impersonate technical support representatives and target Asian Americans who may have limited English proficiency or are less familiar with technology. They use phone calls, pop-up messages, or emails to trick victims into believing their computers have viruses or technical issues. The scammers then gain remote access to the victims' devices, steal personal information, or charge exorbitant fees for unnecessary repairs.
2. **Immigration and Visa Scams:** Asian Americans who are navigating the immigration process or seeking visa assistance may be targeted by scammers. These scammers pose as immigration lawyers or consultants, offering guaranteed visa approvals or faster processing in exchange for upfront fees or personal information. Victims may end up paying for fraudulent services or face identity theft risks.
3. **Romance Scams:** Scammers create fake online dating profiles, specifically targeting Asian Americans looking for love or companionship. They build emotional connections with their victims, often using stolen photos or false identities. Once trust is established, scammers manipulate victims into sending money or providing financial support for various reasons, such as travel expenses or medical emergencies.
4. **Investment and Business Scams:** Scammers may target Asian Americans who are interested in business or investment opportunities, capitalizing on cultural values associated with entrepreneurship and financial success. They offer fraudulent investment opportunities, promising high returns or exclusive deals. Victims may unknowingly invest in nonexistent businesses, pyramid schemes, or fraudulent ventures, resulting in financial losses.
5. **Family Emergency Scams:** Scammers exploit the close-knit nature of Asian families by impersonating a family member in distress. They contact individuals, usually older family members, pretending to be a relative facing an urgent situation or in need of financial assistance. These scams rely on the desire to

help family members and can lead victims to send money or disclose personal information.

How to Avoid:

- Be cautious of unsolicited communications, especially those requesting personal information, financial details, or upfront payments.
- Verify the legitimacy of tech support services, immigration consultants, investment opportunities, or requests for financial assistance before providing any personal information or making financial commitments.
- Educate yourself and others about common scam tactics and red flags to watch out for.
- Encourage open communication within the community to share experiences and warn others about potential scams.
- Report scams to local law enforcement, relevant government agencies, and consumer protection organizations to help protect others and raise awareness.

5 online scams that can target LGBTQ+ individuals:

1. **Catfishing and Romance Scams:** Scammers create fake profiles on dating apps or social media platforms, specifically targeting LGBTQ+ individuals. They build emotional connections and manipulate victims into sending money or providing financial support under false pretenses. These scams prey on the desire for companionship and can result in financial loss and emotional distress.
2. **LGBTQ+-Focused Online Merchandise Scams:** Scammers may create fraudulent online stores or auction listings that sell LGBTQ+-themed merchandise, such as pride flags, apparel, or accessories. Victims may place orders and make payments, but the products never arrive, or they receive counterfeit items of poor quality. These scams exploit the community's desire to support LGBTQ+ causes and representation.
3. **Blackmail and Extortion Scams:** In some cases, scammers may target individuals who are not openly out or have shared sensitive or intimate content online. They threaten to expose this information unless a ransom is paid. This

form of blackmail preys on fear and the potential consequences of being outed, leading victims to comply with the scammer's demands.

4. **LGBTQ+-Based Support and Advocacy Scams:** Scammers may pose as representatives of LGBTQ+-focused organizations, support groups, or advocacy platforms. They solicit donations or request personal information under the guise of supporting LGBTQ+ rights or initiatives. However, the funds may not be used for their stated purpose, and personal information could be misused for identity theft or other fraudulent activities.
5. **Housing Discrimination Scams:** LGBTQ+ individuals searching for housing or roommates through online platforms may encounter scams that exploit housing discrimination. Scammers may post fake listings, explicitly stating preferences or requirements that discriminate against LGBTQ+ individuals. They may request payment for deposits or application fees for properties that do not exist or are not available for rent.

   How to Avoid:

   - Exercise caution when engaging in online relationships or encounters, and be wary of requests for money or financial assistance from individuals you've only met online.
   - Research and verify the legitimacy of online stores, organizations, or advocacy groups before making donations or sharing personal information.
   - Be mindful of the information shared online, especially intimate or sensitive content, and consider privacy settings and security measures on social media platforms.
   - Educate yourself about common scam tactics and red flags, and be vigilant in recognizing potential scams targeting the LGBTQ+ community.
   - Report scams to local law enforcement, relevant online platforms, and LGBTQ+ support organizations to help raise awareness and protect others.

Online Scams and the 2024 Presidential Election

It is important to be aware that major events, such as presidential elections, can create opportunities for scammers to exploit the heightened attention and engagement of the

public. In recent years, there have been instances of online scams and disinformation campaigns surrounding elections, including phishing attempts, fake news articles, and social media manipulation.

Scammers may attempt to capitalize on the political climate, voter engagement, and public interest to deceive individuals and steal personal information, spread misinformation, or exploit political affiliations. It's crucial for individuals to remain vigilant and take steps to protect themselves from online scams during this time.

5 online scams related to political elections

1. **Phishing Emails:** Scammers send emails pretending to be from political campaigns or election officials, asking for personal information, donations, or urging you to click on malicious links.

   Avoidance: Be cautious of unsolicited emails. Verify the sender's email address and cross-check with official campaign websites or contact information. Never click on suspicious links or provide personal information through email. Instead, visit the official campaign website directly.

2. **Fake Fundraising Campaigns:** Scammers set up fake online fundraising campaigns claiming to support a candidate or cause, but they keep the collected funds for themselves.

   Avoidance: Only donate to verified and reputable campaigns. Research the organization or candidate before making any donations. Use official campaign websites or trusted crowdfunding platforms to contribute. Be skeptical of unsolicited fundraising requests on social media.

3. **Voter Registration Scams:** Scammers create fake websites or send emails pretending to be voter registration platforms, tricking people into providing personal information for identity theft or fraudulent purposes.

   Avoidance: Register to vote through official government websites or local election offices. Double-check the website's URL to ensure it is legitimate. Avoid clicking on links in unsolicited emails. Be cautious of sharing sensitive personal information online.

4. **Disinformation Campaigns:** Scammers spread false information through social media, fake news articles, or manipulated images/videos to mislead voters and create divisions.

   Avoidance: Verify information from multiple reliable sources before believing or sharing it. Fact-check news articles and use reputable fact-checking organizations. Be critical of sensationalized or extreme claims. Report false or misleading information on social media platforms.

5. **Robocalls and Phone Scams:** Scammers make automated phone calls pretending to be campaign representatives, pollsters, or election officials, aiming to collect personal information or intimidate voters.

   Avoidance: Be cautious when receiving unsolicited calls. Hang up if the call seems suspicious. Do not provide personal information or financial details over the phone. Verify the identity of the caller by contacting the official campaign or election office through their verified contact information.

   General Tips:

   - Be vigilant and skeptical of any unsolicited communication related to elections.
   - Use strong and unique passwords for your online accounts and enable two-factor authentication.
   - Keep your devices and antivirus software updated to protect against malware or hacking attempts.
   - Educate yourself about common online scams and stay informed about current threats.
   - Report any suspicious activity, scams, or disinformation campaigns to local law enforcement, the Federal Trade Commission (FTC), or the appropriate authorities in your country.

The Technology Behind Scams

Online scammers employ various technologies to commit their fraudulent activities. Here are some common technologies used in online scams:

1. **Phishing Tools and Kits:** Phishing is a prevalent scamming technique where scammers impersonate legitimate organizations to deceive individuals into revealing sensitive information. Scammers use phishing toolkits and software to create convincing fake websites, emails, or messages that mimic reputable companies or services. These tools enable scammers to collect login credentials, financial details, or personal information from unsuspecting victims.
2. **Botnets:** Botnets are networks of compromised computers infected with malware and controlled by scammers. They can be used to carry out a range of malicious activities, including distributed denial-of-service (DDoS) attacks, spamming, or spreading malware. Botnets allow scammers to automate their operations, generate massive volumes of scam messages, or control multiple accounts to execute coordinated scams.
3. **Voice Over Internet Protocol (VoIP):** VoIP technology enables scammers to make phone calls over the internet instead of traditional telephone networks. They can use VoIP services to manipulate caller ID information, making it appear as if the call is coming from a different number or a legitimate organization. Scammers can utilize VoIP to conduct vishing (voice phishing) attacks, pretending to be representatives of banks, government agencies, or tech support to trick victims into revealing sensitive information.
4. **Malware and Ransomware:** Scammers deploy various forms of malware, such as viruses, worms, or Trojans, to infect victims' devices. Malware can be distributed through malicious email attachments, infected websites, or software downloads. Once the malware infects a device, scammers can gain unauthorized access, steal personal information, or deploy ransomware that encrypts victims' data and demands a ransom for its release.
5. **Social Engineering Techniques:** While not specific to technology, social engineering plays a significant role in online scams. Scammers use psychological manipulation and deception to exploit human vulnerabilities and persuade individuals to disclose sensitive information, make fraudulent transactions, or download malicious software. Social engineering techniques can include impersonation, creating a sense of urgency, building trust, or leveraging emotional appeals.

Victims' Psychological and Emotional Damage

Online scams can have significant psychological and emotional impacts on their victims:

1. **Financial Stress and Loss:** One of the primary consequences of falling victim to an online scam is the financial loss. Victims may experience extreme stress, anxiety, and worry due to the financial burden caused by the scam. They may face difficulties in recovering their lost funds, which can lead to long-term financial insecurity and hardship.
2. **Trust Issues and Emotional Betrayal:** Online scams often involve the manipulation of trust and the betrayal of victims' expectations. Victims may feel a profound sense of betrayal, as scammers exploit their vulnerability and deceive them into believing false narratives or relationships. This can lead to a loss of trust in others, making it challenging for victims to form new relationships or trust online platforms in the future.
3. **Shame, Embarrassment, and Self-Blame:** Scam victims often experience feelings of shame, embarrassment, and self-blame. They may blame themselves for falling for the scam, feeling foolish or gullible. Victims might be hesitant to share their experience with others due to fear of judgment or stigmatization, which can further isolate them and hinder their emotional recovery.
4. **Psychological Trauma:** Being a victim of an online scam can result in psychological trauma. The experience of being deceived, manipulated, and financially harmed can have a profound impact on a person's mental well-being. Victims may develop symptoms of anxiety, depression, post-traumatic stress disorder (PTSD), or other psychological conditions as a result of the scam.
5. **Loss of Confidence and Increased Vulnerability:** Online scams can erode victims' confidence and self-esteem. They may question their judgment, decision-making abilities, and become more cautious or skeptical in their interactions. The loss of confidence can make individuals feel more vulnerable and hesitant to engage in online activities or trust others.
6. **Social Isolation and Withdrawal:** Scam victims might experience social isolation, withdrawal, or a reluctance to seek support. They may withdraw from social interactions, both online and offline, due to feelings of shame or a fear of being targeted again. This isolation can further exacerbate the emotional impact of the scam and impede the healing process.

Seeking Support and Recovery

Recovering from the psychological and emotional damages caused by online scams is essential. It's important for victims to seek support from trusted friends, family members, or professional counselors who can provide understanding, empathy, and guidance.

Reporting the scam to law enforcement authorities can also help in preventing similar scams and potentially recovering lost funds.

Victims should remember that they are not alone and that falling victim to a scam does not reflect personal shortcomings. Rebuilding trust, practicing self-care, and developing healthy skepticism when engaging in online activities can aid in the recovery process.

Where To Go If You Become a Victim

If you have fallen victim to an online scam, it's important to take immediate action to minimize the impact and report the incident to the appropriate authorities. Here are some authorities you can contact:

1. **Local Law Enforcement:** Start by contacting your local police department or law enforcement agency. They can document the incident, provide you with an official report or case number, and offer guidance on further steps to take.
2. **Federal Trade Commission (FTC):** The FTC is a government agency in the United States that handles consumer complaints and helps investigate and take action against fraudulent or deceptive practices. You can file a complaint with the FTC through their official website (www.ftc.gov) or by calling their toll-free hotline.
3. **Internet Crime Complaint Center (IC3):** The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). It accepts and analyzes complaints related to internet crimes and scams. You can file a complaint through their website (www.ic3.gov).
4. **Your Financial Institution:** If the scam involved financial transactions, such as unauthorized charges or fraudulent bank transfers, contact your bank, credit card company, or any other financial institution involved. They can guide you on how to report the fraud, dispute charges, and potentially recover lost funds.
5. **Consumer Protection Agency:** Depending on your country of residence, there may be specific consumer protection agencies or organizations that handle fraud and scams. Research and contact the appropriate agency in your country to report the scam and seek assistance.
6. **Online Platforms:** If the scam occurred on a specific online platform, such as a social media site, online marketplace, or dating app, report the incident to the platform's customer support or abuse department. They may have specific procedures in place to address scams and take action against fraudulent accounts.

Remember to provide as much detailed information as possible when reporting the scam, including any relevant documentation, emails, or transaction records. This will assist the authorities in their investigation and increase the chances of identifying and apprehending the scammers.

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 2023 and beyond.