State of Internet Scams 2022

Americans lost a record $6.9 billion to online scams in 2021, up from $3.5 billion in 2019. The amount lost has nearly doubled since the global pandemic began in 2020 as people were forced to work, shop and date online.

This alarming trend is showing no signs of slowing down as an unprecedented number of victims are losing their life savings with many tragically taking their own lives. Moreover, the vast majority of victims are too humiliated to come forward.

The State of Internet Scams 2022 study from Social Catfish offers an unprecedented look into this crisis. The purpose is to inform the public on the most recent scams, how they work, how they can be avoided and the devastating impact they have on the real people who are affected.

This study is an extension of Social Catfish's mission to protect consumers from Internet scams through its reverse search technology which can confirm the identity of the person you are interacting with online.

The company's inaugural State of Internet Scams study released in 2021 became a trusted resource used by consumers, law enforcement, and was cited in the Federal Trade Commission report to Congress titled "Combatting Online Harms Through Innovation"

Methodology

- We analyzed the most recent annual reports released in 2022 by the FBI's Internet Crime Complaint Center (IC3) and the Federal Trade Commission on online scams.
- Social Catfish conducted the largest poll of romance scam victims ever from a private company with 3,047 participants. The poll was conducted from May to August 2022 by email. Respondents are all past romance scam victims and current Social Catfish reverse search subscribers.
- Social Catfish gained insights by working with a reformed Nigerian romance scammer who helps the company investigate scams on the ground in Nigeria. The scammer provided a leaked romance scammer training manual which we include below.

10 KEY FINDINGS FROM THE STATE OF INTERNET SCAMS 2022:

1) **Money Lost to Online Scams Has Doubled Since COVID-19:** A record $6.9 billion was lost to online scams in 2021 according to the FBI IC3. This is up nearly double from $3.5 billion in 2019 before the global pandemic started in 2020. The number of victims also jumped from 467,361 in 2019 to 847,376 last year. Scammers have grown increasingly sophisticated to capitalize on people working, shopping and dating online.

2) **Some States are More at Risk Than Others in America:** According to the FBI IC3, the five states that lost the most money across all types of online scams are: 1/2/3/4/5. The five states that lost the lease

STATE	VICTIMS	TOTAL MONEY LOST	AVG
California	67,095	$1,227,989,139	$18,302
Texas	41,148	$606,179,646	$14,732
New York	29,065	$559,965,598	$19,266
Florida	15,855	$528,573,929	$33,338
Pennsylvania	17,262	$206,982,032	$11,991
New Jersey	12,817	$206,982,032	$15,878
Illinois	17,999	$203,510,341	$10,271
Michigan	10,930	$184,860,704	$16,617
Virginia	11,785	$181,622,993	$14,660
Washington	13,903	$172,767,012	$11,325
Massachusetts	9,174	$157,454,331	$16,3 93
Georgia	11,776	$150,384,982	$12,228
Ohio	17,510	$143,998,767	$7,634
Colorado	10,537	$133,666,156	$12,397
Arizona	12,375	$130,631,286	$10,033
Tennessee	7,129	$124,158,717	$14,583
Maryland	11,693	$103,960,100	$8,476
North Carolina	10,363	$99,110,757	$8,821
Nevada	17,706	$91,416,226	$4,728
Minnesota	5,844	$83,712,410	$14,123
Oregon	5,954	$82,535,103	$12,721
Connecticut	4,524	$75,739,646	$16,020
Utah	4,242	$72,476,672	$15,354
Indiana	11,399	$65,131,003	$5,310
Missouri	9,692	$60,524,818	$5,551
Wisconsin	8,646	$53,797,188	$5,993
Oklahoma	4,156	$51,816,862	$12,078
Alabama	5,347	$50,196,339	$9,262
South Carolina	5,426	$49,522,904	$7,882
Louisiana	4,248	$42,768,322	$9,130
Kentucky	7,148	$ 783,908	$5,310
Iowa	8,853	$37,953,949	$3,820
Kansas	2,693	$33,821,569	$9,666
North Dakota	670	$26,031,546	$31,711
Mississippi	2,170	$21,246,355	$9,483
District of Columbia	2,103	$20,578,948	$9,556
Nebraska	2,407	$20,096,921	$8,202
Hawaii	1,615	$19,743,241	$11,742
South Dakota	951	$18,964,018	$19,065
Idaho	1,882	$18,131,095	$9,396
Arkansas	2,745	$17,682,386	$5,575
New Hampshire	1,487	$15,302,829	$10,291
Delaware	2,132	$15,302,618	$7,055
Alaska	1,787	$15,041,717	$7,314
New Mexico	2,644	$13,070,648	$4,827
Rhode Island	1,205	$12,761,850	$9,287
Wyoming	735	$11,191,079	$13,945
Montana	1,188	$10,249,609	$8,508
Vermont	715	$10,107,283	$13,744
West Virginia	2,135	$9,826,787	$4,428

3) **75% of Romance Scams Victims Are College Educated:** There is a common misconception that people who fall for romance scams must be unintelligent. However, 75% of the 3,074 victims polled by Social Catfish report having some college education and 13% earned graduate degrees. The FTC reported a record $547 million was lost to romance scams in 2021, up from $304 million and labeled it the No. 1 type of fraud.

4) **Middle and Lower Class Americans Make up 84% of Romance Scam Victims:** While lack of education did not increase the likelihood of being a romance scam victim, socio-economic factors did. The Social Catfish poll found 44% of romance scam victims make less than $100,000 and an additional 40% make less than $40,000 per year. In total, 84% of victims earn less than $100,000 and only16% earn six-figures which shows a strong socio-economic correlation that those with less money are more susceptible.

5) **Romance Scams Leading to Financial Ruin:** The Social Catfish poll found 10% of victims lost more than $100,000 with 4% losing

more than $200,000. As noted earlier, 84% of victims earn less than $100,000 annually meaning many had to sell their assets or take out loans to pay their scammers. Moreover, 35% of victims were retired with many having to reenter the workforce.

6) **Tech-Savvy Teens and Children See Largest Increase in Money Lost:** From 2017-2021, victims under 20 have seen a 1126% increase in money lost to online scams, marking the highest increase of any age group over the five year period according to the FBI IC3. This is surprising considering the fact that young people are considered to be more tech-savvy than older generations. This alarming trend may be because 54% of U.S. households polled by Social Catfish do not monitor their children's activities online, leaving them vulnerable to Internet risks.

Teens and Children See Largest Increase in Money Lost in Last Five Years:

AGE GROUP	2017 MONEY LOST	2021 MONEY LOST	PERCENTAGE INCREASE
Under 20	$8.2 million	$101.4 Million	1125.92%
20-29	$67.9 million	$431.1 million	534%
30-39	$156,287,698	937.3 M	499%
40-49	$244,561,364	1.19 billion	386%
50-59	$275,621,946	1.26 billion	357%
60 +	$342,531,972	1.68 billion	390%

Source: FBI IC3 annual reports from 2017 and 2021

7) **Public Losing Confidence in Social Media Platforms as Scams Surge:** The FTC found Americans lost $770 million on scams originating on social media. This marks an eighteen-fold increase since 2017. The poll conducted by Social Catfish found, 41% of respondents think more than 50% of accounts on Facebook and Instagram are fake.

8) **Investment and Cryptocurrency Scams See Largest Annual Increases:** Cryptocurrency and investment scams saw the two largest increases of all scams. A record $1.6 billion was lost to Cryptocurrency scams, a nearly seven-fold increase from $246 million in 2020, while $1.4 billion was lost in 2021 to investment

scams, up from $336 million in 2020, marking a 332% annual increase per the FBI IC3.

9) **Corporations Saw Record Losses to Online Scams:** According to the 2022 IC3 report, corporations reported losing $2.4 billion to business e-mail compromise scams in 2021, marking a 28% increase from 2020.

10) **Elderly Lose Record $1.7 Billion:** According to the most recent data reported to the IC3, in 2021 the number of elderly citizens (aged 60 years or older) who reported being the victim of a scam increased dramatically, with more than 92,000 reporting combined losses totaling more than $1.7 billion. This represents a 74% increase in total losses over the previous year's total.

7 Tips to Avoid Online Scams in 2022

1. **Do not give money** to anyone you have never met in person.
2. **Do not give out personal information** if you have never met in person

3. **Perform a reverse search** using photos, emails, phone numbers and addresses to verify if the person or entity you are speaking to online is who they say they are.
4. **5 big red flags** include poor grammar, refusing to video chat, being in the military, working overseas, asking to be paid in gift cards or cryptocurrency.
5. **Use a password manager** to create many passwords so if one is compromised the rest of your accounts are protected.
6. **Read the Leaked Romance Scammer Training Manual:** To get familiar with their tactics so you can recognize when you are being scammed.

    Available for Download Here:

7. **Report any scam** that you have been a part of immediately to the FTC, IC3, and FBI and your financial institution.

State of Scams 2022

The Evolution of Online Scams

As 2020 drew to a close, Americans were reeling from unprecedented rates of scams and fraudulent activity being perpetrated across multiple different arenas, targeting diverse subsets of the population, and causing innocent victims combined losses totaling in the billions.

Let's take a look at where we were at the end of 2020, and the state of scams over the past year as we work our way through the final half of 2022.

According to data culled from the FBI's Annual IC3 report, 2021 began with Americans having reported 2.8 million cases of fraud or scams costing the victims of these scams combined total losses of $5.8 billion.

While we would love to report that 2020 was an all-time high for scammers engaging in fraudulent activities, unfortunately, the opposite seems to be true. As of the time of this writing, the FBI's most recent IC3 report has been released chronicling the incidences of fraud and scams for the past

year of 2021. Suffice it to say, the situation has not improved. As a matter of fact, it has gotten worse.

What Types Of People Are Getting Scammed?

With the massive increase in internet and telephone-based scams continuing to rise year over year, the FBI, together with the Department of Justice Elder Fraud division, and additional internal and external partner organizations have pooled their resources to create the Internet Crime Complaint Center (IC3) to aid in compiling data and investigating internet scams, their victims, and the total losses in an effort to gain a deeper understanding of who are the most common targets of scammers, and what can be done to help reduce, and prevent future scams.

Since its inception in 2000, the IC3 has received over 6.5 million complaints from victims of scams, at an average rate of more than 552,000 complaints per year, or roughly 2,300 complaints per day. In 2021 alone, victims of reported fraud suffered more than $6.9 billion in combined losses.

The most recent data reported in the FBI's 2021 Internet Crime Report identifies the following segments of the population as the most likely to be targeted, and suffer the greatest losses at the hands of internet scams.

Horrific Internet Crimes Against Children

Young people continue to be the fastest growing segment of the population affected by internet scams. The amount of money lost by young people under the age of 20 rose by 43% last year, amounting to a record $101.4 million up from $70.9 million. This is surprising considering the fact that young people are considered to be more tech-savvy than older generations. But the data suggests that the youth's exposure to technology, particularly social media, is what leads to the increase in susceptibility to scams and other harmful aspects of the internet. In fact, although Gen Z has grown up with technology, a UK study suggests that Gen z is twice as susceptible to online scams as older generations. Many have theorized that this is because of the fact that younger generations are more comfortable sharing personal information online, leading to massive losses.

Child Identity Fraud

Child identity theft affects as many as 1 in 50 children in the US. The average US family loses over $1,000 when a child falls victim to an identity theft scam. What's more, identity fraud targeting children tends to go undetected due to the fact that the child is unaware that the crime is taking place. Even more of a chilling statistic, 73% of children who fall victim to identity fraud know the thief personally.

FBI Warns Caregivers About The Threat of Sextortion Scams Against Children and Teens

The FBI reports a huge increase in the number of reported cases of sextortion scams against children and teens. A sextortion scam is when a scammer blackmails someone online using their sexual images. The scammer will usually demand payment under the threat of exposing their nude images to their friends and family if they do not receive payment or more sexual images. These horrific crimes against the youth often start as catfish scams, with scammers stealing images online, and approaching young kids and teens pretending to be someone of their age. This is a heinous crime with devastating phycological effects, with reports of young

people committing suicide while trying to cope with the shame and humiliation of falling victim to these scams.

What is Contributing to Internet Crimes against children?

One of the reasons that crimes against children are so high is because of the prevalence of children using social media without adult supervision. 9 in 10 family households with internet access have children active on social media, and 54% of households report not monitoring their children's online activities. With children having free reign of the internet without restriction, there are many different risks that they are exposed to, ranging from scams to online abuse. In fact, Global Kids Online conducted a global survey polling for online sexual exploitation and abuse of internet users aged 12-17. They found that the majority of cases where a child is sexually abused online happen through social media, with the most common platform being Facebook, and the most common method of contact being a Facebook messenger.

A study by weProtect found that 54% of respondents were exposed to at least one form of sexual harm online. They also found that the age of first exposure to explicit content online is rapidly dropping. With 18-year-old

respondents reported the average age of first exposure to sexual content online was 12.7 years old. This is a full year earlier than 20-year-old respondents, who reported first encountering this kind of content at 13.4 years old on average.

Other Forms of Harmful Exposure

From surveying children across the world, Global Kids Online also found that a significant percentage of children around the world were also exposed to content about self-harm, suicide, hate speech, cyberbullying, and other forms of psychologically distressing content.

Platforms Posing the Greatest Risks to Children

One of the features of social media platforms that put children at the most risk is platforms that allow a direct messaging feature. The DM feature is almost universal on social media platforms, with the most notable ones being Tiktok, Instagram, Facebook, and Snapchat. With this feature, anyone can reach out to someone they're following, in some cases, anyone who has a public profile can receive a DM from anyone who has an account on the platform. This feature allows many minors to fall victim to fraudulent and illegal activities online.

When Are Children Most Likely To Be Scammed

Children are most likely to be scammed when they are 13 and transitioning into their teen years. This is when their social media usage tends to increase, and they begin to migrate to use messaging platforms like Telegram and Reddit. These platforms tend to be the riskiest platforms for online identity theft, with social media being the riskiest platforms in terms of exposure to explicit content and sexual predators.

Kids Disclosing Scams and Abuse

A survey by Disrupting Harm found that children who fall victim to exploitation are less likely to disclose the harm to their caregivers, with many children preferring to talk to their friends or siblings about the situation rather than their parents, with almost no children going to the police. With only 2.9% reporting reaching out to the authorities. 34% of children told no one at all. Half of these children reported that their lack of disclosure was due to the fact that they felt like they had no one to tell. An additional 10% reported that they didn't tell their parents because they felt that they did something wrong, and feared punishment or disrupting the family dynamic.

When Are Children Most Vulnerable Online

Children are most likely to be scammed when they are 13 when transitioning into their teen years. This is when their social media usage tends to increase, and they begin to migrate to messaging platforms like Telegram and Reddit. These platforms tend to be the riskiest platforms in terms of online identity theft, with Facebook being the most common platform for other forms of exploitation.

Scams Preying On the Elderly

According to the most recent data reported to the IC3, in 2021 the number of elderly citizens (aged 60 years or older) who reported being the victim of a scam increased dramatically, with more than 92,000 reporting combined losses totaling more than $1.7 billion. This represents a 74% increase in total losses over the previous year's total.

One of the reasons for the large number of elderly victims is that scammers deliberately seek out elderly targets for their scams. In the Romance Scammer’s Playbook, for instance, scammers advise preying on victims 35+ because “they have the money they need”. As a consequence, many elderly people who have spent their entire lives putting away savings can

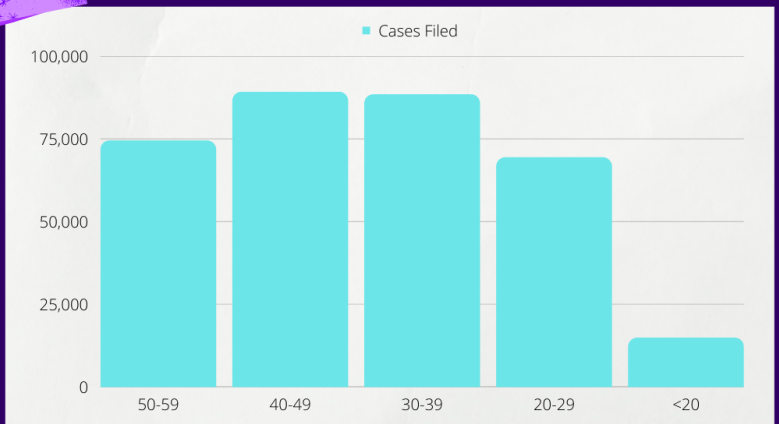
see the money evaporate into thin air in a matter of weeks. The total dollar loss per victim, aged 60 years or older averaged a staggering $18,246.

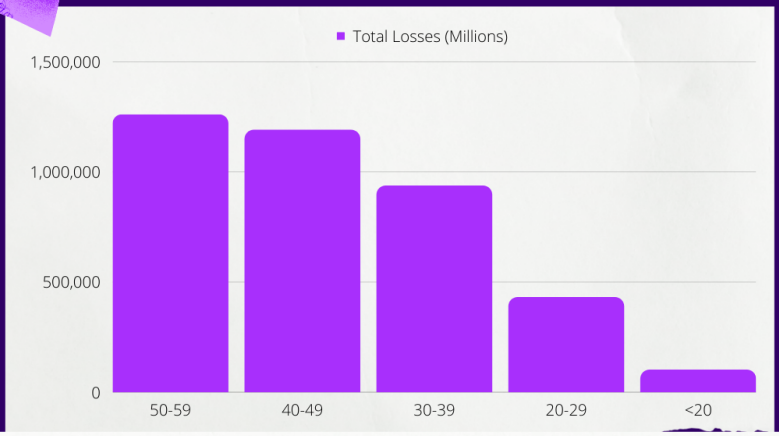
An even more shocking statistic is, 3,133 victims, aged 60 years or older, reported individual losses totaling more than $100,000. One of the most commonly reported scams against the elderly was Tech Support Scams, which claimed 13,900 elderly victims in 2021.

While members of the elderly population are by far the most likely to be targeted and fall victim to scams and fraudulent activity, the demographic groups below also suffered significant losses in 2021.

SocialCatfish.com

Scams by the Age Group





Scam Numbers by Age Groups

- Victims aged 50 - 59 years old filed 74,460 complaints and suffered combined losses of $1.26 billion in 2021
- Victims aged 40 - 49 years old filed 89,184 complaints and suffered combined losses of $1.19 billion in 2021
- Victims aged 30 - 39 years old filed 88,448 complaints and suffered combined losses of $937.3 million in 2021
- Victims aged 20 - 29 years old filed 69,390 complaints and suffered combined losses of $431.1 million in 2021
- Victims aged 20 years and younger filed 14,919 complaints and suffered combined losses of $101.4 million in 2021

Alarming Increase

At the close of 2020, the number of victims of Phishing/Vishing/Smishing/Pharming type internet-based scams hit an all-time high with 241,342 reported cases, up from the 114,702 cases reported in 2019. The numbers have not improved over the past year. The 2021 IC3 report shows that the past year saw an increase to a new record high of 323,972 reported victims of some type of Phishing/Vishing/Smishing/Pharming related scam. Clearly, this is a problem area that must be addressed.

Phishing/Vishing/Smishing/Pharming scams cost victims a total combined loss of $44,213,707 over the past year. While this is a slight decrease from the 2020 combined total loss of $54,241,075, this is not exactly pocket change. So what are the hallmarks of these costly scams, and most importantly how can we stop them and reverse this alarming trend going forward?

Phishing Scams

Phishing, Vishing, Smishing, and Pharming are all terms used to describe the use of unsolicited emails, texts, or phone calls by scammers, and other bad actors whose aim is to deceive the recipient into believing that the communication has come directly from a legitimate company or organization. These communications often request that the recipient provide personal, business, or financial details, or their log-in credentials in order to resolve an issue, or as a matter of routine request. The scammer will then use the information provided to gain unauthorized access to the victim's accounts, and personal or business data.

While improvements in cybersecurity education and awareness have been made to try to inform people about the danger of Phishing/Vishing/Smishing/Pharming activity, there is still much work to do if we hope to reverse this alarming increase in activity by scammers, and other bad actors, and reduce the losses suffered by innocent victims of these scams in the years to come.

The reported number of phishing scams has steadily increased since 2019, with a 182% increase. Phishing scams are mass messaging scams in

which scammers create fraudulent email accounts impersonating a reputable company. They then send out emails to the company's clientele in hopes of getting them to attempt to sign in to a mock version of the real company's website. Once the users have signed in to the fake website, the scammers steal their account information. According to recent research done by IRONSCALES, 81% of organizations have seen an increase in phishing scams since 2020.

Where are People Getting Scammed

Many people get scammed on social media, but this is far from the only place where scammers reach out to their victims. The platform that victims are contacted on depends on the type of scam that scammers have in mind. 23% of romance scams take place on Instagram for instance, but commerce scams tend to take place on selling platforms like eBay or Craigslist.

Many of the scams on these platforms involve the scammer receiving money for a product, and never actually shipping it. With this in mind, there has been an increase in scams on social media stemming from platforms rolling out new shopping new features that allow people to buy and sell

products directly on the social media platform. These scams range from products being far lower quality than advertised, to orders never arriving at all.

A Record $770 Million Lost to Social Media Scams

One of the most common starting places for internet scams is social media. A common tactic for social media scammers is to steal images from influencers in order to create fake profiles online. These fake profiles are then used to reach out to people on social media for various types of scams. A total of $770 million was lost to social media scams in 2021. About 925 of the reported 2021 fraud losses indicated that social media was the contact method. What's more, adults ages 18-39 were 2.4 times more likely to have their scam initiated on social media.

Of investment scams, 54% of them were initiated on social media. 36% of the scams that originated on social media started on Instagram, whereas with romance scams, 13% of scams were initiated on Instagram and 23% were initiated on Facebook.

What Types of Scams Are Happening On Social Media?

One of the newest types of scams happening on social media is shopping scams. With social media platforms rolling out features that allow users to sell products, many consumers are falling victim to scams without recourse to receive their money back. These factors represent a 72% increase in money lost due to non-payment non-delivery scams.

One of the most common starting places for internet scams is social media. As previously mentioned, scammers steal images from influencers in order to create fake profiles online. These fake profiles are then used to reach out to people on social media for various types of scams. A total of $770 million was lost to social media scams in 2021.
About 925 of the reported 2021 fraud losses indicated that social media was the contact method. What's more, adults ages 18-39 were 2.4 times more likely to have their scam initiated on social media.

Why Are People Getting Their Images Stolen

A key feature of most internet scams is appropriated identities. Scammers steal images from social media accounts online, only to repost the images under a fake account using a made-up name. The people in these stolen photos range from ordinary people to influencers and models. The fake

accounts that the scammers set up using these photos are then used to reach out to thousands of potential victims all across the internet in everything from investment scams to romance scams.

What Makes Someone a Target to Get Their Photos Stolen?: Many people who get their images repeatedly stolen experience a massive disruption to their lives due to the fact that people continually reach out to them about the scams they've suffered, many still under the impression that they have been talking to the real person. The people who have had hundreds of fake accounts made using their images have a few things in common:

SocialCatfish.com

Why Are People Getting Their Images Stolen?

They are considered to be attractive

Scammers steal images from attractive people because most people are far more likely to answer a DM from someone with supermodel looks. And once they engage them in conversation, they use all of their manipulation tactics to reel them in.

They tend to have jobs that require them to travel overseas

Oil rig scammers, soldiers, engineers, and doctors in the Peace Core are all scammer's favorite fake identities. This is because they can come up with excuses for meeting someone because it will blow their persona.

They have pictures of them doing a wide variety of activities

Because scammers have to convince someone that they are real, they steal photos from people who have pictures of them doing a wide variety of activities. This makes it appear as if they're actually living their life while talking to the person online.

Semi-Popular

They often have notoriety within a small community on the internet or a sizable social media following but are typically not "famous"

socialcatfish.com

Although many people who have their images stolen aren't considered famous, it is common for people to believe they are talking to real celebrities online. From country music stars to movie star Keanu Reeves, there are fake accounts that reach out to people and convince them that they want a relationship but need their help to pay some unexpected expenses. Usually using the excuse of having a controlling and overbearing manager who doesn't allow them to have access to their real accounts. Although most people who continually have their photos stolen fall into the above categories, the patterns differ based on the gender of the person whose identity is being impersonated. For fake profiles featuring men, many fake accounts focus on people who are emphasizing their lifestyle or influence, and approach people with investment opportunities, or engage women in a relationship and then try to get them to buy into a "lucrative business deal" or to help with an emergency. Many fake accounts featuring women, on the other hand, often involve beautiful influencers and focus on the physical appearance of the model in order to attract men.

Why Do Scammers Steal So Many Photos?

Studies have shown that attractive people are seen as more trustworthy than people who are considered to be unattractive, so stealing images from

an attractive influencer may make the target of the scam more likely to interact with them.

Where are People Getting Scammed

Many people get scammed on social media, but this is far from the only place where scammers reach out to their victims. The platform that scammers are contacted on depends on the type of scam that scammers have in mind. 23% of romance scams take place on Instagram for instance, but commerce scams tend to take place on selling platforms like eBay or Craigslist. Many of the scams on these platforms involve the scammer receiving money for a product, and never actually shipping it.

Facebook Scams

Users on Facebook seem to be especially susceptible to the pitfalls of the internet. As mentioned above, according to one of the largest polls conducted on romance scam victims, 26% reported that they met their scammer through Facebook. This is likely due to the fact that users on Facebook tend to be older than users on other social media platforms, with the average age of Facebook users being 40.5 years old, and romance scammers prefer to target older people because they have enough money

saved to exploit in their scams. Despite Facebook having an older user base, a large percentage of children around the world who reported experiencing abuse and harassment online reported being engaged by their abuser on Facebook. Like romance scams, much of this abuse comes from catfishing scams and people creating fake accounts using fraudulent identities.

Facebook lottery scams:

A Facebook lottery is where scammers hack into the Facebook accounts of someone and send messages to their friend list in order to ensnare them in this scam. These scams are particularly devastating because they exploit the trust that a victim has in their friend, family member, or a reputable company. These scams aim at eliciting information from people by getting them to give up personal information such as bank account details. Many of these scams even claim that in order to receive the lottery winnings, the target will have to pay the taxes and fees upfront.

How to spot these scams: Facebook sites lottery scams as among the most common scams on their platform. Facebook says that they have never run a lottery or sweepstakes, and they never will. So if anyone is

approached on the platform claiming that they won a lottery, it is definitely a scam.

Have Scammers Gotten Away With These Scams?

Although some scammers outside the US have been extradited to the United States for prosecution. Many scammers can get away with these scams because they are located overseas. Because of this, law enforcement agencies in the United States have a difficult time locating these scammers and bringing them to justice.

2021 Saw a Massive Jump In Investment Scams

Money lost to investment scams jumped a mind-boggling 332% this past year, with investors losing $1,455,943,193 to investment scams according to the FBI IC3.

BEC Scams

Business email compromise scams (or BEC scams) are spoofing scams in which scammers steal or memic an email address of a member of an organization whose position is in finance. They then convince other

members of the company to do a wire transfer to the account they control. Upon receiving the transfer of funds, the scammer pockets the money and then disappears. This was the most costly scam in 2021, with losses reaching nearly $2.4 billion. (23.), a 28% increase from last year.

Scammer's Methods of Payment

Gift Card Scams

Many internet scams involve gift cards. Scammers get people to send them gift cards online under many false pretenses. They may request payment for a fake service, to cover basic expenses, or as a favor to get them out of a fake emergency.

The reason for scammers requesting gift cards is that they are an easy way of transferring money overseas while hiding the transfer from authorities. Because of this, this is one of the preferred methods of payment along with bitcoin. In fact, 1 in 4 people says the scam was initiated when a scammer asked them for a gift card. In fact, according to the FTC, gift cards are the most commonly reported method of payment to scammers. Once someone reads off the number on the back of a gift card to a scammer, the scammer now has access to the funds on the cards.

How Do Gift Cards Scams Work

Gift card scams are most commonly initiated through a phone call. It is a form of a phishing scam where the scammer will call people impersonating a customer support rep from a reputable company. They then ask you to read the numbers off the back of the gift cards. They usually refer to the numbers as a “security code” when in reality, the only purpose of this number is to access the money on the card. Once the person reads off the numbers, scammers have access to the funds on the account.

Most Common Gift Cards To Stay Away From

There are a few gift cards that scammers ask for more than others. The common gift cards requested by scammers are Target gift cards. Other gift cards commonly used in scams are Google Play cards, Apple, eBay, Walmart cards, and Steam Cards. Scammers like directing their victims to buy these gift cards because they are easily available in most stores, and gaining access to the money on the card is as simple as getting the person to read off the numbers on the back of the card.

Money Lost To Gift cards

Although it might sound like gift card scams may involve minimal amounts of money, losses of over $5,000 have increased by 14% in 2021. In 2021, Americans lost more than $148 million to gift card scams, with a median income of $2,500.

Cryptocurrency Scams

Cryptocurrency is one of the preferred methods of payment for scammers. This is because cryptocurrency is difficult to trace back to an individual, and many of the victims they scam are not familiar with cryptocurrency, so the scammer often walks them through the process of sending the money, giving them more control over the situation, which often leads the scammer to have access to all of the victim's funds.

Bitcoin is one of the most commonly used cryptocurrencies in scams. Part of the reason it is so commonly used is likely the fact that it is the biggest and most well-known cryptocurrency in the world.

Pig Butchering Scams

Pig Butchering is a type of scam where scammers agree to invest money for the victim, they usually put the money into an “investment website”, which is usually a fake website that mimics an investment account. Once they make the initial investment for the victim, they will see the account balance grow, signaling that they have made a good initial return on the investment. Because of this, their confidence grows and they are willing to invest more money. They will even send money back to the victim, encouraging them to invest more and more into the account, and once the investment is at its peak, they take their money and head for the hills.

Getting Your Money Back

Once you convert your money to Bitcoin, getting it back can be extremely difficult. This is because Bitcoin is largely anonymous. Since cryptocurrency is a new technology, some tech companies are working with law enforcement to develop technologies to trace the money and identify individuals who are using the technology for fraud and money laundering activities.

How Do Scammers Get Away With These Scams

Scammers get away with these scams in a variety of different ways, but what makes it difficult to track back to them is two main things.

Payment: Scammers typically use methods of payment that are difficult to track. Some of the most common methods are gift cards, cryptocurrency, and money laundering tactics that make it difficult to track back to them.

Communication: Scammers tend to use methods of communication that make it difficult to find their true identity. Social Media accounts can typically be created using minimal pieces of information and stolen identities. They also use VOIP numbers to communicate over the phone, which makes it difficult to trace them.

Why are Some People More Susceptible to Scams

Some people are more susceptible to scams due to a few factors. One of the factors that lead to susceptibility to scams is a lack of understanding of how the internet works. Many victims of scams are unfamiliar with concepts like catfishing, phishing, and other common scam activities. The other type of scam has to do with tragic life conditions. In our video series Scamfish,

many people who fall victim to romance scams are people who are going through tragic life circumstances such as a death in the family, loss of employment, or a divorce. This loss typically causes them to either seek love to fill the void on dating apps or be more likely to reply to someone who reaches out to them. In the context of romance scams, one of the biggest contributing factors to the likelihood of someone falling for a romance scam is whether or not they have fallen for a romance scam in the past. Although this is counterintuitive. People who have fallen victim to romance scams in the past are more likely to fall victim to another scam in the future.

Gaming Scams

Although social media is a common way people are scammed, gaming platforms are another very common method of first contact used by scammers. This is because scammers can often initiate contact in these platforms without their targets giving it a second thought. Scammers often come up with scripts and standard ways of getting their victims from game chats to messaging apps to prolong the conversation in an attempt to build a sense of familiarity that they can exploit in their scams.

Statistics of Gaming Scams: The number of gaming scams grew by 68.6% between 2010-2021, with the number of reported scams growing by 32.6% between 2020-2021.

The technology used in these scams: The technology used in gaming scams tends to be smartphones, gaming consoles, messaging apps, and gift cards. All of these methods of communication and payment transfers offer some form of anonymity or pseudo-anonymity for the scammer, making it difficult to trace back to them.

The games that scammers scam on range from simple online games like Words-With-Friends to popular console games like Roblox and Fortnight. Gaming scams are often a scam of confidence, meaning the scammer starts communicating with the victim, usually via a game chat, and they begin to befriend their target in seemingly casual interaction. Once the conversation has been extended, scammers look to solicit personal information such as banking credentials, social security numbers, and any other piece of information they can leverage to gain access to the victim's funds. Many of these gaming scams turn into scams of confidence, such as romance scams or investment scams.

Why Do Victims Fall For These Scams: Victims tend to fall for these scams because they don't expect to meet a scammer on these platforms. Often, when victims meet a scammer in places that pertain to their hobbies, they recall not expecting someone to enter the space with the intention of taking advantage of them. Because of this, many victims are blindsided by these scams.

Dating Apps

The two main types of scams that occur on dating apps are investment scams and Romance scams. Oftentimes the scam is a combination of both. The hit Netflix show The Tinder Swindler illuminated the issue of romance scams, However, the problem is often more complex than the specific instance illustrated in the documentary. Instead of interacting with people using their true identities, scammers often construct personas with a combination of other people's photos and fabricated stories. Dating apps are among the most common places for scammers to make contact with potential victims and initiate their scams under an alias and stolen photos.

Many of the romance scam victims we interview in our documentary series Spamfish report being contacted first by their scammer after meeting on a

popular dating app like Tinder, Plenty of Fish, or Facebook Dating, and quickly being asked to move the conversation to a messaging app. This is because many dating apps like Tinder make it more difficult to create an account to prevent fakes and other fraudulent activities. So if their account is reported, they will be barred from rejoining the platform on the same device. As a result, scammers quickly suggest moving to apps like Google Hangouts or Facebook Messenger where there are less stringent guidelines.

Tinder

Being one of the largest dating sites out there, Tinder has its fair share of scams. But, as mentioned, Tinder takes some precautions to make sure that the people on their platform are real, and that people who have been found to be engaging in fraudulent activities on the platform are not welcomed back on. However, as the Netflix Documentary Tinder Swindler shows, The platform still isn't flawless. Tinder has a verification feature that prompts users to go through a series of poses to verify that it is really them in the photos. Once the photos are processed, the users will get a blue checkmark on their profile signaling to other users that they are real people. The blue check mark wears off within a few weeks, and the user will have

to go through the same process to regain their verified status. The issue with this process is that it is completely optional, and briefly swiping through Tinder will reveal that the majority of users opt not to use this feature.

Furthermore, the format of a dating app like Tinder makes it more difficult to spot a fake profile because of the superficial nature of the dating app itself. Users are given a few pictures and a brief bio to decide whether or not they “like” someone. And once they like them they are free to engage in conversation.

Messaging Apps

Messaging apps are one of the most common methods of communication with a scammer. Because many scammers field their victims on social media, they’ll move them to a messaging app to further communicate with them. Scammers moving the conversation to a messaging app occurs almost immediately after the first interaction. Victims commonly report the original account they were in contact with on social media disappearing or blocking them. Scammers also prefer conversation on messaging apps because after the scammer gets all of the money they can from their

victims, they block them and the victim has no recourse for getting their money back or finding the true identity of the person behind the scams.

How to Spot A Fake Profile

There are a few ways you can spot a fake dating profile. Generally, “catfish” profiles impersonating males tend to be different from those impersonating females. Profiles impersonating males tend to focus more on the career they’re in, and the lifestyle they’re living, whereas female catfish profiles often feature provocative language and racier photographs. To get an idea of what is meant by this, go to a major sports page on Instagram for instance, and scroll through the comment section on any given post. You’ll immediately encounter dozens of fake profiles with provocative language designed to ensnare men in various types of scams. One of the surest ways of spotting these accounts is by looking at their follower-to-like ratio. They tend to have a lower follower count and be following far more people than are following them.

Why Do Scammers Scam People

There are two main reasons scammers scam people. Oftentimes these scammers are from foreign countries where there is less economic

opportunity. In Lagos Nigeria, for instance, many young men turn to internet scamming to make money because they find it hard to find gainful employment opportunities within their communities. Also, it has become a part of the culture in some capacity. They can find mentorship, support, and advice on how to best carry out their scams. There are even criminal enterprises dedicated to organizing and coordinating these scams.

The second answer to why scammers scam is more straightforward. Scammers scam to achieve one of a few ends. They will scam to steal your identity, and bank information, or even get you to unknowingly launder their money for them, thus committing a felony offense. Scammers will often turn people into money mules under false pretenses. Depending on how deeply they can sink their hooks into a victim, they may scam a single person in all of these ways. And once they have no more financial assets left and banks have banned them from banking with them, they will get them to take out loans and send them the money. What really makes a scammer so dangerous is they're master storytellers, and they will get their victims to believe that they are doing the right thing by breaking the law and illegally moving money for them.

The Devastating Impact of Romance Scams

Many victims of scams report experiencing psychological distress. Generally, victims report feelings of shame and humiliation, but these emotions intensify depending on what type of scams they fell victim to. Romance scams, for instance, can take an extraordinary toll on their victims. This is because the victim's sense of betrayal is heightened in this particular scam because of the romantic and often intimate aspects of the interaction between victim and scammer. Victims often share their deepest hopes and dreams with their scammer. Throughout the whole interaction, scammers carefully craft their persona to be in alignment with the victim's deepest desires for the future. They use the knowledge of these desires in their manipulation tactics. Since the scammers often claim to be multi-millionaires living abroad, their promises include purchasing a house in a location where the victim has always wanted to live, paying off their mortgages, and even gestures like taking care of the person’s family members and children from a previous relationship.

With these deviously crafted personas and these perfectly tailored promises, the romance scammer can proceed to extract tens of thousands of dollars from their victims. Some of the emotional scars run so deep that

even after the victim comes to terms with the fact that they have been scammed and the person they are talking to is not real, they will continue communication or the “relationship” with the scammer. One woman is quoted as saying “I know he is a romance scammer, but he is just so romantic that he’s ruined every other man for me”. These sorts of emotions are commonplace, with many victims getting locked in an endless cycle of being contacted by, and falling victim to romance scammers. Many are aware of the likelihood that their e-sweetheart is a scammer, but they elect to indulge in their romantic fantasy with the charmer with bad intentions regardless.

Since it takes very little time to set up a social media account, and an even shorter amount of time to download and repost images from a popular influencer or good-looking user on a social media site, scammers can endlessly retarget victims. Armed with the knowledge of the target’s desires and life goals learned from their interactions with the victim under the pretenses of their previous persona, the scammer has an enhanced ability to deceive and manipulate the victim with the newly crafted persona. In fact, some romance scammers that have reached out to Social Catfish’s team have referred to a “VIP List” which, is a list of victims who have

proven themselves willing to pay large sums of money in the past, and who can be retargeted through a different account using yet another set of stolen images. In fact, earlier this year, the social catfish team demonstrated how a fake Instagram account can be created in less than 5 minutes, and it can be used to endlessly target victims on the Internet. So if a victim rebukes a romance scammer, they can construct a new persona complete with a new set of social media accounts to re-engage with the victim in no time.

This endless cycle of deception and artificial romance often destroys victims financially and emotionally. Romance scammers will take every penny that the victim has, and once the victim has no money left, they will prompt them to take out loans, second mortgages, and even borrow money from their family and friends, all fueled by false promises and a sense of urgency created by fabricated emergencies. The financial devastation combined with the separation and tension the scams tend to create in their family lives often drives victims into isolation and deep depression.

What makes the sense of isolation victims feel even worse is that many people in the world cannot relate to their stories. This is because romance

scam victims are at the forefront of this global phenomenon, and most people cannot fathom how someone can fall deeply in love with someone they've never met, and oftentimes have never even had a phone call with. A good framework to help people understand how this could be is that of a romantic novel. Romance scammers are like novelists carefully crafting the character of their target's dreams in real-time. They can do this so effectively that long after the victim discovers it is a scam due to many failed attempts to meet in person or video chat, and warnings and interventions from friends and family, they are unable to exit the situation because they have become addicted to their interaction with the character the scammer has created.

Romance Scams Victimizing Single Educated Women

Romance scams overwhelmingly target women, with 78% of respondents being female, 44% making middle income, and 75% possessing some form of a college education. In addition to many victims being educated career women, romance scams have a heavy impact on women from the ages of 35 ranging all the way up to the elderly years. This is because romance scammers strategically and systematically target single women of these

ages based on the belief that “they are desperate for love”. And they have enough savings for romance scammers to con them out of.

Young People of Color Hit Hard By Romance Scams

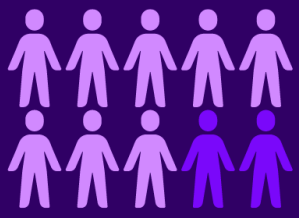
Although romance scams are an issue that affects everyone, young people of color are hit especially hard when compared to their white counterparts. For caucasian people, romance scams are largely a problem affecting the middle-aged and elderly, but in the case of people of color, people under the age of 40 are disproportionately affected by romance scams.

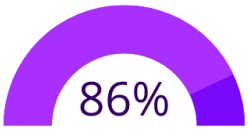
SocialCatfish.com

Scam Demographics

The **female** majority

78% of victims are female.
Only 22% of victims are male.





Low-income hit hard.

86% of victims make fall under middle or low income.

Romance Scams Thrive on **Facebook**

27% of romance scam victims say their scam was initiated on Facebook.

96% of White victims were over the age of 40.

Dating Sites a **Hot Bed** For Romance Scams

35% of victims say they met their scammer on a Dating site.

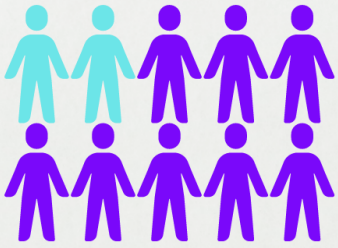
3X

Young people of color 3x as likely to be scammed.

13% of POC victims were under 40. Young white victims only account for 4% of the total white victims.

The Upper End of the **Financial Devastation**

Nearly 2 in 10 victims sent $100,000 or more.
1 in 25 sent over $200,000.



Despite this large amount of money, many of these victims are middle-class people who sold their assets or taken out loans in order to send the money or retired elderly people who sent their entire life savings to the scammer they fell in love with online.

How To Recover From These Scams

After years of working with countless victims, we've discovered that the first step in the process of recovering from a romance scam is to terminate all communication with the scammer and former romantic partner. We recommend that the victim blocks the scammer outright on all platforms. This is because romance scammers are master manipulators, and if the victim leaves the tiniest crack in the door, the scammer will find a way to be let back into their life. Many romance scam victims say they're done, but are seeking "closure" through a confrontation with the romance scammer, but this is not advisable due to the fact that the scammer will never relent. Romance scammers generally seek payment at all costs. They will even reveal their "true identities" which may or may not be who they actually are. But regardless, it is most often just another ploy designed to emotionally manipulate the victim. At Social Catfish, we have a saying "the scam never ends". This is because no matter how the scam develops, or what is said by the scammer, the end goal of the interaction is always payment. No matter how dire the financial or legal situation gets for the victim of the scam, regardless of the physical, emotional, or psychological state of the victim the scammer will not relent. "The scam must go on". They will seek

payment to the last penny while draining the victim of all emotional and financial resources.

How to Report These Scams

One of the most important things when it comes to slowing the increase of scams we're seeing on a yearly basis is to increase the reporting of scam-related incidents. It is estimated that 85% of online fraud goes unreported, meaning the true number of scam victims and money lost is certainly even more staggering than is currently known. In order for government agencies to properly prevent these scams, the full scope of the problem must be understood. Many people who fall victim to online scams feel helpless and are searching for a way to get back at their scammer, and there is only one, the true way of doing so. The steps to getting back at your scammer go as follows:

Getting Your Money Back

Once you convert your money to Bitcoin, getting it back can be extremely difficult. This is because Bitcoin is largely anonymous.

Since cryptocurrency is a new technology, some tech companies are working with law enforcement to develop technologies to trace the money and identify individuals who are using the technology for fraud and money laundering activities.

How Do Scammers Get Away With These Scams

Scammers get away with these scams in a variety of different ways, but what makes it difficult to track back to them is two main things.

Payment: Scammers typically use methods of payment that are difficult to track. Some of the most common methods are gift cards, cryptocurrency, and money laundering tactics to make it difficult to track back to them.

Communication: Scammers tend to use methods of communication that make it difficult to track back to them. Social Media accounts can typically be created using minimal pieces of information and stolen identities. They also use VOIP numbers to communicate over the phone, which makes it difficult to track back to them.

How to Get Back at a Scammer

One of the most important things when it comes to slowing the increase of scams we're seeing on a yearly basis is to increase the reporting of scam-related incidents. It is estimated that 85% of online fraud goes unreported, meaning the true number of scam victims and money lost is certainly even more staggering than is currently known. In order for government agencies to properly prevent these scams, the full scope of the problem must be understood. Many people who fall victim to online scams feel helpless and are searching for a way to get back at their scammer, and there is only one, the true way of doing so. The steps to getting back at your scammer go as follows:

How to Get Back at a Scammer

1 Report the Account

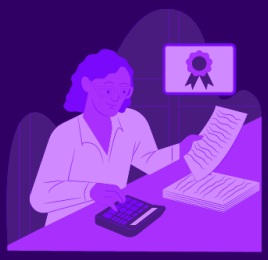
Reporting the account to whatever platform you were in contact with will help prevent the scammer from contacting anyone else through that account.

2 Collect all of the information you have on the scammer

Getting every piece of info you have on the scammer in order will help the law enforcement agencies effectively investigate the crime.

3 Report the scam to the IC3

Once you report a scam to the IC3, an analyst will review the case and send it to state and federal law enforcement agencies.



4 Contact the Consumer Protection Agency (if it is a business)

The consumer protection agency is designed to protect consumers from fraudulent and predatory activities by businesses.

Why are Some People More Susceptible to Scams

Some people are more susceptible to scams due to a few factors. One of the factors that leads to susceptibility to scams is a lack of understanding of how the internet works. Many victims of scams are unfamiliar with the concepts like catfishing, phishing, and other common scam activities. The other type of scam has to do with tragic life conditions. In our video series Scamfish, many people who fall victim to romance scams are people who are going through tragic life circumstances such as a death in the family, loss of employment, or a divorce. This loss typically causes them to either seek love to fill the void on dating apps or be more likely to reply to someone who reaches out to them. In the context of romance scams, one of the factors that seem to be a contributing factor to the likelihood of falling for a romance scam is having fallen for a romance scam in the past. Although this is counterintuitive. People who have fallen victim to romance scams in the past are more likely to fall victim to another scam in the future.

Where Do Scams Come From?

Scams come from all over the world, and certain scams are characteristic of certain regions. This is because scammers in these regions exploit

certain cultural expectations or have a support system for advice on how to carry out particular scams.

Nigeria

Many internet scams originate from Nigeria, specifically Lagos. Oftentimes, these scams aren't coming from a single individual with an internet connection, but rather a criminal enterprise that is organizing and coordinating efforts to make their scams believable. The organization then launders the funds obtained. One of the reasons for the prevalence of scams in this area is the poverty that many Nigerians live under. According to the World Bank, 40% of Nigerians are living below the poverty line and an additional 25% of people are at risk of falling below the poverty line. Because of this, many of the country's best and brightest turn to cooking up schemes to scam people on the internet. Many victims of scams report feelings of shame because of the fact that they were tricked out of their money online, feeling that it shows a lack of intelligence on their part, but when you consider the fact that many of the scammers have the intellectual capacity to be doctors, lawyers, or even scientist if given the right access to

opportunity, it's no wonder their scams are often so well crafted and devastating.

Another reason so many internet scams come from Nigeria is it has become part of the culture in many respects. As an example of this, a young Nigerian man we interviewed reported having difficulty finding employment after graduating high school, but he knew people in his community made a living by romancing women online and getting them to send them money. This influence was enough to get this particular youth into this line of work. There is also guidance on the tactics and techniques to use, as well as advice on selecting their targets and masking their country of origin through adaptation to cultural norms. Scammers often understand the cultural differences in certain areas. For instance, Taiwan is reporting a romance scam issue, and in these scams, scammers are exploiting the geopolitical tensions between the island and mainland China, and concocting stories that require payment because of these tensions.

China

Despite the large strides the country has made in recent decades, a large portion of China's population is still living in poverty. And poverty in a region

seems to be a factor in the prevalence of scams. Scams in China tend to target businesses by exploiting cultural expectations. For instance, one of the most prevalent scams occurs when a scammer contacts a company and claims that they are looking to make a large purchase with their company. They then tell them that it is customary for the company to send gifts and throw a banquet when doing such a large business deal. Through this story, they get the company to send money to cover the cost of the banquet and to send gifts. Then the scammer disappears. This has become known as the “come to China” scam.

Paper tiger scams are another scam targeting businesses coming out of China. These are scams where a Chinese business reaches out to a company and claims to be well connected within the government and industry they work in. This scam is not aimed at getting the company to send money per se, but these are exaggerations designed to get more favorable terms in their contract negotiations. The reason these scams work is that the due diligence report will uncover that it is, in fact, an actual business, but the claims they make about their connections are exaggerated, making them appear to be larger and more connected than they are in reality. Hence the name “paper tiger scam”.

Eastern Europe

Many scams also originate from eastern European countries. Many phishing scams, for instance, can be traced back to this region. Of the top 5 countries sending the most phishing emails, all five of them were from Eastern Europe, namely Lithuania, Latvia, Serbia, Ukraine, and Russia.

Eastern Europe is also known for its cyber-attacks. These attacks can either be politically motivated, targeting government organizations and critical infrastructure. or simply aimed at stealing credit card information.

The War in Ukraine

Google threat analysis called TAG has been monitoring the scammer's use of the war in Ukraine to lure people into opening malicious emails and clicking harmful links. They have observed shifts in behavior targeting users with new variants of computer viruses aimed at installing software to steal passwords through Cookies. Many of the scammers committing these attacks are known by their screen names, as authorities track their crimes by these names and attempt to tie them back to their true identities.

https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/

The Technology Behind Internet Scams

The technology behind online scams varies from scam to scam. But generally, scammers use the following technology to carry out their scams:

- **Smart Phone:** Many scams are initiated and carried out through the scammer's smartphones. From these phones, scammers are able to download various applications in order to carry out various aspects of these scams.
- **Social Networking Apps:** Social networking apps give scammers a nearly unlimited number of people to target for their scams. From Facebook to Instagram, there are thousands of fake accounts aimed at ensnaring people in these scams.
- **Messaging Apps:** Messaging apps are a common method of communication used by scammers. This is because setting up an account on a messaging app is relatively easy and requires little to no information that can be used to identify the scammer. Furthermore,

many messaging apps are customizable. Meaning scammers can use the app while still using their fake identities.

- **VOIP Numbers:** A VOIP number (short for voice over internet protocol) is a digital number that scammers use to make phone calls over the internet. These numbers are nearly indistinguishable from real phone numbers, but offer anonymity for scammers, as the number cannot easily be traced back to their true identities.
- **Gift Cards:** Gift Cards are often used in scams to transfer money because they are nearly untraceable. Meaning it is an easy way for them to launder money while remaining anonymous and flying under the radar of government authorities.
- **Cryptocurrency:** Cryptocurrency is another common payment transfer method among scammers, specifically bitcoin. This is because bitcoin is anonymous, making it extremely difficult to trace a transfer back to an individual. Furthermore, many of the people online scammers are targeting don't understand the technology behind cryptocurrency. This means that scammers have a better chance of deceiving and manipulating their victims when it comes to receiving payments.

How To Avoid These Scams

Avoiding online scams has a lot to do with separating the real from the fake. This means identifying the real person, business, or products that the scammer is proposing to sell. By identifying what is real, you can clearly see what is designed with the intention to scam. We have broken this up into three separate categories to illustrate how to best avoid being scammed on the internet.

1. Scams of Confidence

A little-known fact is that the phrase “con man” is short for “confidence man”. A scam of confidence occurs when a scammer assumes a fraudulent identity and engages with someone with the intention of scamming them. Online, scams of confidence most often involve creating a mock website or email address pretending to be a reputable company or stealing someone else's images and operating under an alias. The best way to avoid a scam of confidence is to find the real person or entity that the scammer is impersonating. If someone appears to be a stock trader, online retailer, or love interest, analyzing the photos they're using could help illuminate the truth. Products like a reverse image search can help you find the name and

profiles of the real person, and if the information doesn't add up, you can safely conclude that the person is a fraud.

2. Shopping Fraud

Shopping fraud can be avoided in a few ways. The first way is by verifying the seller, particularly if the seller is a reputable brand, such as Amazon or Walmart (online). Many scammers appropriate the domain names of these companies, so the name of a scam website will closely resemble that of the real website. Double checking the domain name of the real service versus the fake one is a sure-fire way of spotting a scam. Scammers may exploit spelling differences, spelling errors, and other minor discrepancies to deceive people into buying something from their fraudulent website. This is known as typosquatting. Checking for spelling errors in a URL is a great way of avoiding fake websites.

3. Advance Fee Scams

Advance fee scams occur when a scammer online demands a fee upfront before delivering a product or providing a service. In some cases, they

claim to have a large sum of money tied up in a legal case, a bank account, or even an inheritance that needs taxes or lawyer fees before the money can be dispersed to the victim in the fashion of the classic “Nigerian Prince Scam ". In 2021 alone, $98,694,137 was lost across 11,034 reports to advanced fee scams.

What Platform Are These Scams On?: Mass messages are one way for scammers to lure people into their scams. Another way for people to get scammed is through social engineering. This is because advance fee scams often occur after scammers make promises for repayment. These advance fee scams are often created out of a sense of urgency to make the situation seem dire, making the victim believe that them sending the money in time can help the scammer protect themselves against an impending disaster, or that there is a limited time to close the deal for the victim to claim their reward for their contribution.

How To Avoid This Scam: Because scammers go to considerable lengths to make the deal seem appealing, it’s important to assess whether or not it seems too good to be true. If the person finding you and reaching out to you with this offer seems like it would be unlikely under legitimate

circumstances, you should consider the possibility that you are being targeted by a scammer. And like many other scams, if the scammer requests payment in the form of cryptocurrency or prepaid cards, it is likely a scam.

Threats and Harassment

Many of the scammers commit these scams through coercion under the threat of various acts. Some of these threats can be overt, such as threats of violence against victims and their families, or they can threaten persecution under the law, posing as a government agency. These scams can be broken out into a few subcategories.

Statistics: There were 12,346 total reports in 2021 that fall under the category of threats of violence with a total of $4,390,730 in total losses.

4. E-Commerce Fraud

The fourth way of avoiding an internet scam is by checking the images of the products an E-commerce store is claiming to sell. This can be achieved through a reverse image search. A reverse image search can be run by taking a screenshot of the photo and uploading it into a reverse image

search bar. This will help you assess the quality of the other websites the product is listed on to make an informed decision as to whether or not the e-commerce brand is trustworthy enough to buy from. This search should be run alongside a general search on the reputation of the domain.

Covid's Long-Term Effect on Internet Safety

With the rise of Covid-19 in 2020, the internet saw an unprecedented rise in scams. This is likely due to the fact that more people than at any other time in history were spending time on the internet in lieu of real-world activities due to the quarantine protocol. With the influx of people on most Social Media platforms, scammers saw this as an opportunity to capitalize. 2020 saw a record number of internet scams, with Americans losing a record $4.2 billion. With an increase in scams this year totaling $5.8 billion, it seems that the pandemic may have been the catalyst for a bigger issue that our society will be forced to contend with in the years to come.

The steady increase in scams can be attributed to the fact that many people have become accustomed to carrying out their social interactions through the internet, with the number of internet users ballooning during the

pandemic, many people who may not have been as tech savvy as individuals who spent a lot of time on the internet in the pre-pandemic era, making it more difficult for these individuals who were not familiar with concepts such as phishing, catfishing, and more, to spot and avoid online scams.

PPP Scams

The pandemic also set the stage for new types of scams involving citizens taking advantage of government aid meant to alleviate the suffering that the pandemic caused for many business owners. The program was known as the PayCheck Protection Plan (or PPP). It is estimated that around 15% of the $800 billion issued by this program was fraudulent. Over 900 criminal investigations were opened as of December 2021, with many perpetrators facing charges of bank fraud and wire fraud, carrying a maximum penalty of 30 years in prison and a $1,000,000 fine.

Unemployment Scams

Unemployment scams are another outlet that many people used to abuse government programs designed to help people during the pandemic. It is

estimated that $20 billion lost to scams in 2021 in California alone. It is estimated that a total of $87 billion was lost to fraud across all states. This issue becomes even more glaring when considering that Arizona believes that up to 30% of the unemployment benefits issued were subject to fraud.

Laws in States or Countries That are Stopping/Slowing Down Scams

Scammers have many tools at their disposal these days. They could constantly call you on the phone in hopes that you accidentally give up some information to them. They could send you a legitimate-looking email and steal your information or plant a virus. Even your dating apps aren't safe as some profiles are falsified just to get your information while you are in hopes of finding your true love. With scammers being so prevalent in our digital age, governments have been working hard to keep up with new technologies and how to protect their citizens from becoming victims of scams. But which states or countries have actually tried to pass legislation to limit scams?

State Laws

At the State level, some laws have passed but without much of a federal guide, it has been hard for some states to pass any hard-hitting laws against scammers. Most states only prohibit unsolicited commercial messages but that hasn't stopped spammers from robocalling you or sending you fake emails. There really is no legal action taken against scammers if you fall victim to one of their message campaigns.

Arkansas SB514

Only Arkansas has passed a law that aggressively goes after scammers with their State Bill 514 which makes spoofing a felony that could be punishable with up to six years in prison. This law also requires telecommunication companies to report to state regulators that they are actively utilizing new technologies to block spam calls. Other than that most state laws follow in line with the federal government's laws against scammers.

Federal Laws: CAN-SPAM

In 2003, Congress passed the CAN-SPAM Act that required the FCC to issue rules and regulate commercial emails a**iler**

Social Catfish is an award-winning people search and verification company committed to helping people avoid online scams and fraud. Americans lost a record $5.8 billion to online fraud last year.

Since being founded in 2015 by David McClellan with a $65 personal investment, the southern California-based company has helped 50 million website visitors confirm if the person they've met online is really who they claim to be.

The reverse search engine uses proprietary technology – including artificial intelligence, blockchain tracking and facial recognition – to verify images, social media profiles, phone numbers, emails, and more.

Social Catfish was an Inc. 5000 honoree and recognized in 2020 as the No. 118 fastest growing company in America and over the last three years the company has grown by 766% and is on pace for $14 million in revenue in 2022.

Social Catfish works with high levels of law enforcement to help track down online scammers to help victims recover their money. Their inaugural State of Online Scams 2021 Study was cited on page and mobile messages. However, federal law has yet to be changed since 2003 to meet modern needs against Robo-callers and online scammers.

International Law

International Law isn't that different from the U.S. The FBI has worked with other international investigation agencies to stop scammers and protect foreign travelers from becoming victims, but they still leave most of the precautions up to you.

Corporate Prevention

The real strides against robocallers and scammers come from companies that are developing technology to proactively protect their customers. T-Mobile began reporting and identifying spam calls for their customers and every cellular company has followed up with their own protections. Most phone companies have introduced technologies that screen strange phone numbers to avoid direct contact with scammers. Email companies have filters that will take out spam mail and potentially dangerous email messages. Some companies are working with the federal government to implement new technologies to further protect the public and create new regulations that will limit the power of scammers.

State of Scams Projections

With technology becoming an increasingly important aspect of our lives and internet scams reaching historic heights, the future of online interaction is uncertain. In this section of The State of Scams, we endeavor to take on the monumental task of predicting how internet scams and other online threats will shape our society, and what individuals and government representatives can do to take on these challenges.

A Continued Increase in Losses to Internet Scams

Technological innovation is expected to bring the majority of Earth's population to the internet in the coming years. It is estimated that over 60% of people on the planet will be online by 2025. That is over 5 billion people. Companies such as Elon Musk's Starlink are aimed at global adoption of the internet, with the high-profile company aiming to have the entire planet connected by a network of satellites by the end of this decade. This includes members of the first world, as well as populations in the developing world. This increase can have two primary effects on the current internet ecosystem.

1. **The number of overall internet users will increase**, creating more innovation worldwide, and more money to be spent on eCommerce brands worldwide, opening up more economic opportunities for all.
2. **A proportional increase in bad actors online.** There will likely be an increase in the number of people looking to take advantage of people joining the increasingly ubiquitous use of the internet. This is likely to increase scams such as phishing, identity theft, romance scams, and investment scams to name a few.

With such large-scale adoption of the internet by cultures all over the world, there are likely to be great strides in innovation, for local populations, as well as humanity as a whole. However, with a large increase in people on the internet, will come a large amount of sensitive data that scammers are looking to take advantage of.

Security Threats in Everyone's Home

The internet of things is a concept in technology where companies aim to create "smart appliances". Which are devices that are connected to the internet, and typically use some form of artificial intelligence to provide value to their users. Examples of this technology include appliances such as Alexa, Roomba, smart TVs, and even smart cars like Tesla. But these

convenient devices come with a potential downside. Since they exist on the internet, they are potentially vulnerable to infiltration by scammers and other bad actors.

Privacy Risks of the Internet of Things

A real illustration of the potentially devastating impacts that fraud and other cyber attacts can have on personal smart device users was an iCloud hack that happened in 2014 where the nude photos of high-profile female celebrities, such as Jenifer Lawrance leaked to the entire internet. 89% of young women report having taken nude photos on their devices in the past. So the celebrity nightmare scenario is a real world possibility for the average person today. As we move more of our love lives online, the issue of personalized online security will become even more essential.

Another chilling example of the vulnerabilities of smart technology is an instance where a family's home security system was hacked. Hackers spied on the family through their own webcams, they even spoke to the family's young daughter through one of the devices, and taunted and tormented the family throughout the house's home security system as they fled the home in terror. Just a few years ago, this might have sounded like

the plot of a bad movie, but today, this increasingly becomes a threat that many households across the world will be forced to contend with.

These hacks have the potential to put the information of users of these devices at risk, but in a world where smart devices are beginning to drive our cars and lock and unlock the doors to our homes, cyber attacks also have the potential to put users' physical safety at risk.

Attacks On Population Centers

In 2021, a hacker nearly poisoned California's water supply, simply by knowing the password of a former government employee. This hack could have affected millions of people. What's more, After the poisoning of the water supply was prevented, the hacker got away without having his true identity revealed. This near-disaster was made possible with a simple hack. Something as precious as a state's water supply can be compromised by simply knowing login credentials. This story highlights the potentially devastating consequences of a small breach in security. It is a perfect illustration of how the increasingly connected world will demand increased security on every level. From individual security to family security, and home security, as well as the security of the precious resources that population centers rely on. Technology has come to play a critical role in

the proper functioning of our cities, meaning it is absolutely imperative to secure them against attacks.

Threats To Civilians by State Actors

Another potential cyber threat that increases as a result of the world's population becoming increasingly dependent on the internet is cyber warfare. This includes acts of antagonism due to geopolitical tensions, such as the alleged Russian hack on the Ukrainian power grids that took place on Chrismas 2015 and on the same day the following year in 2016. Cyber warfare is becoming an increasing threat to global population centers, as hostile powers can use cyber warfare to attack critical infrastructure, wreaking havoc on unsuspecting population centers. The US even accuses Russia of attempting to hack a nuclear power plant.

Although our reliance on internet connectivity opens us up to large-scale attacks, there is also the potential for attacks targeting individuals, with dozens of documented instances of governments stealing the data of citizens of rival nations, sometimes aimed at achieving ends that are unknown.

The Increased Risk of Bot Farms

Bot farms are organizations that create mass amounts of fake accounts on social media in order to push propaganda as well as harass and scam users on these platforms. Bot farms became a topic of discussion in 2016 with questions about their influence on the 2016 US Election through Facebook. In the past, these bots amounted to little more than an inconvenience, but in the near future, they may become even more difficult to spot due to AI. As stated throughout this report, a key tactic employed by online scammers is stealing identities, but in the future, highly sophisticated online personas can be made in seconds through AI. Although this may sound far-fetched, some form of this technology already exists, and it is publicly available online. For instance, a website called "This Person Does Not Exist" can generate fully authentic-looking fake images of people in less than a second. Eliminating the need for scammers to appropriate images belonging to real people. Making it more difficult to find out if an identity is authentic. In addition to this, an automated writing software technology called GPT-3 is an AI that has advanced language capabilities and is open to the public. Scam prevention is often about verifying authenticity, but variations of these technologies threaten to muddy the

waters between what is real and what is fake online, posing a massive risk to internet users.

What is Social Catfish?

Social Catfish is a consumer protection company dedicated to illuminating the problem of internet fraud and minimizing the often devastating impact they have on individuals and society. We work to put names and faces to the tens of thousands of people who have their lives and finances significantly impacted by the epidemic-level rise in internet scams we've experienced in recent years.

The third danger of scams is the harm to one's mental health. This should seem intuitive, seeing as how financial ruin leaves everyone in a shoddy mood – to put it mildly. However, Chris Lees thinks that scams and mental health might be part of a vicious cycle. "We found that people with mental health problems are three times more likely than the rest of the population to have fallen victim to an online scam. This increased risk means that a majority (61%) of online scam victims have also experienced a mental health problem" (Money and Mental Health Policy Institution, 2022). So not only do scams lead to mental sickness and stress on your brain, but stress on your brain can also make you more vulnerable to scams in the first

place. This means that we must be extra-cautious whenever we venture online.

What is Social Catfish?

Social Catfish is a consumer protection company dedicated to illuminating the problem of internet fraud and minimizing the often devastating impact they have on individuals and society. We work to put names and faces to the tens of thousands of people who have their lives and finances significantly impacted by the epidemic-level rise in internet scams we've experienced in recent years.