Scams for 2019

Airbnb Scam

Amazon Fake Order Cancellation Emails

If you get an email about an order cancellation from Amazon.com, there's a good chance it's a scam. Click on links in the email and you could unintentionally download malware onto your device. Or you might be sent to a site that aims to collect your Amazon account information, like your username and password. If you receive such an email and recently placed an order, go to Amazon.com to check your order status.

Apple Care Scam

This new smartphone scam uses phishing emails to send Apple users to a fake Apple website. iPhone users receive a pop-up image of a system dialog box that tells users their phone has been "locked for illegal activity." When users click on the link, scammers enroll them into a fraudulent "mobile device management service" that allows scammers to send malware apps to iPhones. Read more here about phishing scams and how to spot them.

"Can You Hear Me?" and "Yes" Calls

This scam happens when you answer the phone, and the person on the other line asks: "Can you hear me?" and you respond, "Yes." Your voice is being recorded to obtain a voice signature for scammers authorize fraudulent charges over the phone. You can visit the FCC website to block any unwanted calls. The BBB Scam Tracker received more than 10,000 reports on the "Can you hear me?" scam, but none of the reports resulted in an actual loss of money.

Car Scams

The FBI shared information on a growing scam in which crooks target people looking to buy cars and other vehicles online. The FBI has received 26,967 complaints with losses totaling $54,032,396 since tracking this issue from May 2014 through December 2017. This car scam starts with a criminal posting an online advertisement with a low price to get the attention of a buyer, including photos of the vehicle and contact information. When a buyer reaches out, the "seller" sends more photos and what appears as a logical reason why the price is discounted and indicates a need to sell.

The criminal then instructs you to purchase prepaid gift cards in the amount of the sale and share the prepaid codes. You're usually told you'll receive the vehicle in a couple of days, but victims never hear from the scammers again.

Cryptocurrency Scams

As the price and popularity of Bitcoin and other cyber-currencies skyrocketed in late 2017, scammers eagerly sought to take advantage of the frenzy. The Japanese Bitcoin exchange Coincheck was hacked in January, and the thieves were able to steal more than $500 million in cryptocurrencies. This is the largest cryptocurrency hack to date. Facebook and Instagram have banned advertisements for certain bitcoin, initial coin offerings (ICOs), and some other cryptocurrency-related products because of deceptive and misleading practices. Several ads were leading victims to sites such as Prodeum, whose only purpose was to take their money and not provide the advertised service.

Death Threat Hoax

The FBI has warned consumers about death threats being made through emails that state "I will be short. I've got an order to kill you."

The email then demands money or bitcoin as a payout from the email recipients. Other versions of the scam could state that a "hitman has been hired to kill" them. This scam is very aggressive and threatening in nature to convince people that they have to pay or else.

Fake Bank Apps

Scammers will spoof the apps of big banks in order to separate you from your money. A recent survey by Avast, a multi-national cybersecurity firm, found that one in three worldwide users mistakenly believed that a fake mobile banking app was the real thing, putting their financial data at risk. Thieves use the big customer base of major banks to try to get past the secure app stores and collect personal information.

Fortnite Scam

Fortnite: Battle Royale has more than 125 million players worldwide, and that tremendous pull extends to hackers and scammers too. Players and parents should pay attention as Fortnite creator Epic Games is warning gamers about the most common Fornite scam involving "free V-bucks." Scammers offer free or discounted v-bucks, the in-game currency, to help players elevate their game. What can result in identity theft, downloading malware on a device or having your money stolen.

Gift Card Scams

The BBB is warning people about emails offering help to check their gift card balances. If you receive one of these emails, do not click open or click links within. Scammers use these emails websites in order to get your card number and PIN in order to drain your account. The BBB offers the following tips to avoid gift card balance scams:

- Go to the retailer's website: If you need to check a gift card balance, go to the site listed on the back of the card itself. If there is none, go to the website of the company and look for a link to the gift card page.
- Use gift cards right away: A good way to avoid scams and other issues is to simply use gift cards soon after you receive them.

- Examine the gift card before buying: Before purchasing a gift card, be sure to give it a thorough look to make sure the PIN isn't exposed, or the packaging hasn't been tampered with.

- Register your gift card with the retailers: If the retailer allows the option to register your gift card, take full advantage. registering your gift card makes it easier to keep track of any misuse occurring, that way you can report it sooner and potentially end up saving the money that is stored.

Grandparent Scam

This scam has been around and has seen an increase in activity of late. Depending on who answers the phone call, the person on the other line will say, "Hi, Grandpa" or "Hi, Grandma" pretending to be the grandson or granddaughter of the older victim. The scammer then tells them a story that ends with, "I need money right away to… (insert issue here—pay my traffic ticket, post bail, pay for an ambulance)." All of this is said without providing too many details. If pushed, the scammers will say things like "please don't tell Mom or Dad" or "My nose is broken, so I may sound strange." Victims can end up wiring money to the scammers as a result. Read more here about other senior scams.

Home Improvement Scams

Another common seasonal scam centers around home improvement. As the weather gets nicer, homeowners often look to improve their homes. The Better Business Bureau says in 2017, there were nearly 350 home improvement scams reported to BBB Scam Tracker across the U.S., resulting in more than $600,000 lost. Some scammers go door-to-door, offering to do improvement projects. They may take a deposit, and then never complete the work If you're not sure the salesman is legit, you can ask for a card and get back to them once you have been able to research the company by visiting the BBB website. These scams can also happen after major national disasters — hail storms, tornadoes, hurricanes, mudslides, and fires, among other things.

Instagram Fake Ads

It can be difficult to tell what's real or not on social media these days—including advertisements. Scammers often post fake ads to get you to buy one product only to send you a cheap knockoff. Instagram has offered some tips if you think you have come across a suspicious ad:

- You can learn more about an account if you go to their profile, tap the menu and then select "About This Account." There, you can see the date the account joined Instagram, the country where the account is located, accounts with shared followers, and username changes. Within "About this Account," you can also see all ads that the business is currently running.

- People can report an account, an ad, or a post that they feel is misleading. To report an ad, click the "..." on the top right of the ad and click Report Ad. Follow the on-screen instructions and select "It's a scam or it's misleading."

- You can always go back and visit your own ad interactions, including all ads you have clicked on in Stories and Feed, from the past 90 days within your Settings.

IRS Scam

Whether you have received your tax refund check by now, are waiting on an extension from the Internal Revenue Service or are just starting to prepare your taxes, be on alert for scammers. The IRS, state tax agencies and the nation's tax industry are warning taxpayers to be on the lookout for scams as "a surge of new, sophisticated email phishing scams" are being reported. The holidays and tax season present great opportunities for scam artists to steal valuable information through fake emails the IRS states. They want consumers to watch out for email schemes that try to fool you into thinking they're from the IRS or partners in the tax community. In 2018, the IRS noted a 60% increase in bogus email schemes that seek to steal money or tax data.

The tax season can also see threatening scam calls from fake IRS agents. These fake agents usually demand money from victims or state that they will be arrested. The IRS has stated publicly that the summer is when the calls usually increase. The calls can also be recorded messages left on your

voicemail that leave the impression that if you do not call back, the IRS will issue a warrant for your arrest. It's important to note that the IRS does not ever call or leave urgent messages asking you to call them back. Taxpayers can forward these email schemes to phishing@irs.gov—then hit delete.

Jackpotting

Jackpotting is a new cyber-attack scam that the Secret Service warned financial institutions about criminals installing software or hardware on ATMs that force the machines to issue large amounts of cash. Criminals have found ways to exploit the standalone machines commonly found in pharmacies, big-box retailers, and some drive-thru ATMs. It's hard to know the exact financial implications because sometimes these crimes aren't disclosed publicly, but anytime money is missing, it's sure to have an impact on the banks and ultimately you—the consumer—in the former of higher fees or more obstacles to accessing your cash.

Jury Duty Scams

Another new spoofing phone call scam has popped up and involves scammers posing as judicial officials or police and calling people to let them know they failed to report for jury duty and owe a fine. Scammers can spoof law enforcement phone numbers or names so people receiving the call may think that the call is legitimate. The FBI in Atlanta has received numerous complaints about the scam from people in and around the Savannah, Georgia area.

Medicare Card Scam

The Federal Government mailed out new Medicare cards that now have an 11-digit identification number instead of an enrollee's Social Security number to help protect seniors from identity theft. About 59 million people will receive the cards with a requirement from Congress that the Centers for Medicare & Medicaid Services remove Social Security numbers from Medicare cards by April 2019.

Because of the update, scammers are taking to the phones to try trick people into giving them their new 11-digit identification number so they can take over their identity. According to an Allianz survey, the elder financial abuse victims average loss was $36,000.

Netflix Scam

The popular streaming service is the target of an email phishing scam featuring the subject line "payment declined," which may get your attention if you are a subscriber. The email wants you to click on a link to update your credit card information. If you see this don't click on the link because it can be dangerous malware. Visit your Netflix account by typing the address in yourself to check your account as a safer means of verifying your account status. The Federal Trade Commission (FTC) issued a warning to consumers about emails being sent requesting updated payment info. Netflix has stated that customers can get more info to protect themselves against phishing scams and other malicious activity at netflix.com/security or by contacting its customer service department directly.

The FTC also said consumers can report phishing scams at ftccomplaintassistant.gov or by forwarding them to the agency's spam@uce.gov address and to reportphishing@apwg.org, which is used by the Anti-Phishing Working Group, a coalition of internet service providers, security vendors, financial institutions, and law enforcement agencies. In addition, the FTC recommends alerting Netflix, by forwarding the message to phishing@netflix.com.

No Roof Scam

With summer upon us, thunder, hurricanes, and hailstorms can wreak havoc. If you recently suffered damage to your roof from weather events, be wary of people coming to your door offering their repair services as these storms can bring out the worst in people. These scammers will make false promises to people needing to repair or replace their storm-damaged roofs. Many times they will ask payment before they start working or the job is completed. The BBB has partnered with cities on a campaign called the "No Roof Scam" to help consumers spot roofing contractor fraud.

Patrick Dempsey Scam

This scam is anything but McDreamy, as the popular Grey's Anatomy actor Patrick Dempsey has publicly stated that he has an online impersonator on the loose. The scammer is asking his fans and others through social media to send money to him for his Maine-based nonprofit. The scam has been going on for a while as fraudsters keep setting up fake accounts to send messages hoping to find victims that will send them money.

Porting Scams

The scam called "porting" involves criminals stealing your phone number and your phone service in order to get access to your bank account through confirmation text messages.

Scammers start by collecting your name, phone number and then gather any other information they can find about you such as your address, Social Security number, and date of birth. Then they contact your mobile carrier and state that your phone has been stolen and ask that the number be "ported" with another provider and device. Once your number has been ported to a new device, scammers can then start accessing your accounts that require additional authorization such as code texted to your phone.

Romance Scams

Though Valentine's Day is over, romance scams will continue to pop up throughout the year.
A romance scam typically involves a criminal setting up an account on a dating site with fake information and photos for a profile that is too good to be true. Once a target has been established, the scam usually escalates to the thief's unveiling of a money problem. Typical scenarios include the request for funds so he or she can travel to meet you in person or to help a sick relative.

Unfortunately, seniors are the primary targets for romance scams, since they often spend more time alone as they age. Romance scams cost Americans more than $230 million as nearly 15,000 people were conned in 2016, according to the Federal Bureau of Investigation.

Secretary of State Scam

This scam starts when you receive an email claiming to be from former Secretary of State Rex Tillerson, who says you're owed a payment he knows about because of an investigation by the FBI and CIA. The scam reportedly states that you will receive an ATM card with more than 1 million dollars on it, but first you have to send $320 along with personal information to receive it.
The Federal Trade Commission (FTC) says this is false, warning Americans to not fall for this—or anytime you're told you have won a prize, owe money, or may go to jail.

Shimmer Scams

A shimmer scam is an update on skimming except that thieves are using "shimmers" to target chip-based credit and debit cards. A shimmer is a very thin piece of paper that can read your card number and access your credit or debit card's EMV chip—the chip designed to help make your card more secure.

DID YOU KNOW? A shimmer is a very thin piece of paper that can read your card number and access the EMV chip on your credit or debit card.

A thief will put a shimmer into an ATM and let it collect information from each card that is used, allowing them to create a non-chip version or magnetic strip credit card then. Shimmers have been showing up more recently despite first being reported on in 2015. In 2017, the number of debit cards compromised at ATMs and merchant card readers—typically via skimming devices that capture card data—rose 10%, according to FICO.

Tax Arrest Scam

The Internal Revenue Service (IRS) recently warned the public about "sophisticated phone scams" targeting taxpayers by claiming to be IRS employees. The scammers demand that the victims owe money to the IRS and to pay them promptly or be arrested, deported or have their driver's license suspended. Sometimes, the caller becomes aggressive, warning people that a Sheriff or local law enforcement will show up at their door if they don't pay immediately. The IRS warning also

reminded consumers that the IRS would never call to demand immediate payment over the phone, threaten to bring in local police, ask for credit or debit card numbers over the phone, or require you to use a specific payment method for your taxes.

Tax Prep Scam

Not only are U.S. taxpayers the targets of scammers this tax season, so are the tax professionals that prepare tax returns. Tax fraud is big business for fraudsters that can steal the tax preparers information and turn around and sell it on the dark web for money.

This year scammers are sending a lot more phishing emails in an attempt to gain access to the accountant's computer. By doing so, the scammer can get access to that tax professional's client list and computer IP address to file fake tax returns on their behalf. Once submitted, the scammer will have the refund check sent to an address that they can pick up the check.

Tech Support Fraud

In 2017 there were 11,000 complaints related to tech support fraud that resulted in claimed losses of nearly $15 million—an 86% increase in losses from 2016. These tech support scams have prompted the Internet Crime Complaint Center (IC3) to warn consumers about criminals claiming to provide the customer, security, or technical support as a cover in an effort to defraud individuals.

The scam can take place through a phishing email, phone call, pop-up ad or even a locked screen on your device with a phone number to call to fix. The IC3 offers several tips and guidance on how to handle situations like this and reminds people that legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals.

Ticket Scams

Looking for tickets to a concert or for that upcoming football game? If so, beware of tickets scams. The prevalence of online ticket sellers and resellers has created plenty of ticket scam opportunities that you need to be wary of when you go to buy your tickets. The BBB Scam

Tracker reported more than 300 ticket scams reported last year with the most common scams center around reselling fake or non-existent tickets posted on online classifieds and price gouging.

If possible, try to purchase from venue or pause to verify the source of where you are buying the tickets. Discounted prices may be too good to be true. You can look up sellers on The National Association of Ticket Brokers to confirm the site is a verified reseller. Also, make sure to the site is a secured site or used a protected payment option in credit cards versus cash, debit cards or wire transactions, so you have a better chance at getting your money back if scammed.

Veterans Scams

Fake charity scams are nothing new, and the Veterans Affairs Department and the U.S. Postal Inspection Service warns that veterans of the armed forces are particularly vulnerable. The scammers reportedly offer pension buyouts to veterans or ask veterans to donate to a charity that sounds and looks real but isn't. The scammers take the donations or cash the pension checks.

The scammers will also take the donor's personal information to create a new fake identity or commit more crimes under that person's name. According to an AARP survey, 16% of veterans have lost money to fraudsters, compared to 8% of non-veterans.

"Your Order Has Arrived"/Shipping Status Scam

You may have received an email that says your "order" from Amazon or other ecommerce retailer has arrived or has been shipped. It likely asks you to click on a link. These emails can be a phishing scam attempting to get personal information from you by asking you to confirm your bank information or other information only known to you. If you are unsure about an email, make sure to check the actual email address to see if it from the company it says its from. Usually phishing scams will say the company name "Amazon," but when you click on the email address, you'll notice it's not from an Amazon domain. Also, you should never send personal information to an email address without confirming first that it is a legitimate business. You can always visit the

retailer's website directly and log in to your account to confirm any issues or call their customer service number on their main website.

How to Protect Yourself From Being Scammed?

To avoid being scammed, you have to remain diligent and follow these steps:

- Assess the validity of all messages that you receive from people and business that you do not know. That includes any unsolicited phone calls, people knocking on your door, emails sent you—even those that look like they are from a company you do business with, or family and friends—and letters received in the mail that look like they are official.

- Any emails and links sent to you that seem off should be checked first, by rolling your cursor over them with your mouse before actually clicking on the link. Look at the destination URL is to see if it looks legitimate or not.

- Scammers will also pose as imposters from businesses or organizations and call or approach you in person. The Consumer Financial Protection Bureau (CFPB) recently warned people about scammers posing as CFPB employees.

Criminals will go to great lengths to try to pressure you with demands for money or payments. If you feel you are being victimized, make sure to report the scam to the proper government agency, your local Better Business Bureau office, and your local police department.