The Ultimate List of the Year’s Worst Scams
by Matt Tatham

Airbnb

This scam starts with an impostor home or apartment owner directing the renter to a fraudulent website to finalize the payment. The renter is left without the money and without a place to stay.

“Can You Hear Me” and “Yes” Calls

This scam happens when you answer the phone and the other person asks: “Can you hear me?” and you respond, “Yes.” Your voice is being recorded by scammers to authorize fraudulent charges over the phone.

Car Scams

This scam starts with a criminal posting an online advertisement selling a car with a low price to get the buyer’s attention. When the buyer reaches out the criminal instructs the buyer to purchase prepaid gift cards and share the codes. Buyer is told the car will be received in a couple of days but is left without the money and the car needed.

Cryptocurrency Scam

With the popularity of Bitcoin and other cyber-currencies scammers are eagerly to take advantage of this opportunity. The Japanese Bitcoin exchange Coincheck was hacked in January and the thieves were able to steal more than $500 million. Facebook and Instagram have banned advertisements for certain Bitcoin and other crypto-currencies.

Death Threat Hoax

This is an aggressive scam by e-mail that demands money or bitcoin to be paid or they will kill you. The FBI came out warning consumers about this type of threat.

Fake Bank Apps

Scammers posing as banks in the forms of apps to collect personal information from customers.

Home Improvement Scams

Scammers go door-to-door, offering to do improvement projects. They may take a deposit and never complete the work. If you’re unsure ask for a card and do a research on the business by visiting the BBB Website.

Jackpotting

Is a new cyber-attack scam in which criminals install software or hardware on ATMs forcing the machines to issue large amounts of cash. It has an impact on consumers in the form of higher fees and more obstacles to access your cash.

Jury Duty Scams

Phone call scam in which scammers pose as judicial officials or the police calling to notify you that because you failed to report for jury duty you owe a fine.
Medicare Card Scam

The Federal Government issued new Medicare cards to replace the SSN for an 11-digit number to help protect seniors from identity theft. With this new update scammers are calling people and tricking them into giving the 11-digit number. Elder financial abuse victim’s average loss was $36K.

Netflix Scam

This popular service is the target of an e-mail phishing scam featuring the subject line “payment declined”. The e-mail wants you to click on a link to update your credit card information. This can be dangerous malware.

Porting Scams

The scam called “porting” involves criminals stealing your phone number and phone service to get access to your bank account through confirmation text messages. Scammers collect your personal information and contact your mobile carrier and state your phone has been stolen and ask the number to be “ported” to another provider and device. Scammers then start accessing accounts that require additional authorization such as code texted to your phone.

Romance Scams

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. The scam escalates to the thief’s unveiling of a money problem or the request of funds to travel to meet you in person. Seniors are the primary targets, romance scams cost Americans more than $230 million.

Secretary of State Scam

This scam starts when you receive an email claiming to be from Secretary of State Rex Tillerson, who says you’re owed a payment he knows about because of an investigation by the FBI and CIA. You have to pay $320 and send your personal information to receive an ATM card with more than $1 Million dollars.

Shimmer Scams

A thief will put a shimmer into an ATM to collect information from each card that is used, allowing them to create a non-chip version or magnetic strip credit card. A shimmer is a very thin piece of paper that can read your card number and access your credit or debit card’s chip.

Tax Arrest Scam

The IRS recently warned the public about 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. The IRS reminded consumers that they will 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. Scammers are sending 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

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 Internet Crime Complaint Center offers several tips and guidance on how to handle situations like this and reminds people that legitimate customer service, security, or tech support companies will not initiate unsolicited contact with individuals.

Veterans Scams

The scammers 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.

Source: Experian.com