SCAMS and SCAMMERS

Common Scams Observed at the University of Minnesota

Compiled by:
University of Minnesota Police Department

Adapted from:
(https://www.consumer.ftc.gov/scam-alerts)
10 Things You Can Do to Avoid Fraud

Crooks use clever schemes to defraud millions of people every year. They often combine new technology with old tricks to get people to send money or give out personal information. Here are some practical tips to help you stay a step ahead.

1. **Spot imposters.** Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request — whether it comes as a text, a phone call, or an email.

2. **Do online searches.** Type a company or product name into your favorite search engine with words like “review,” “complaint” or “scam.” Or search for a phrase that describes your situation, like “IRS call.” You can even search for phone numbers to see if other people have reported them as scams.

3. **Don't believe your caller ID.** Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is genuine.

4. **Don't pay upfront for a promise.** Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, or a job. They might even say you've won a prize, but first you have to pay taxes or fees. If you do, they will probably take the money and disappear.

5. **Consider how you pay.** Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through services like Western Union or MoneyGram is risky because it's nearly impossible to get your money back. That's also true for reloadable cards like MoneyPak, Reloadit or Vanilla. Government offices and honest companies won't require you to use these payment methods.

6. **Talk to someone.** Before you give up your money or personal information, talk to someone you trust. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, do an online search, consult an expert — or just tell a friend.

7. **Hang up on robocalls.** If you answer the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal, and often the products are bogus. Don't press 1 to speak to a person or to be taken off the list. That could lead to more calls.

8. **Be skeptical about free trial offers.** Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. And always review your monthly statements for charges you don’t recognize.

9. **Don't deposit a check and wire money back.** By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If a check you deposit turns out to be a fake, you’re responsible for repaying the bank.

10. **Sign up for free scam alerts from the FTC at ftc.gov/scams.** Get the latest tips and advice about scams sent right to your inbox.
Scammers can fake caller ID info

May 4, 2016
by
Andrew Johnson
Division of Consumer and Business Education, FTC

Your phone rings. You recognize the number, but when you pick up, it’s someone else. What’s the deal?

Scammers are using fake caller ID information to trick you into thinking they are someone local, someone you trust – like a government agency or police department, or a company you do business with – like your bank or cable provider. The practice is called caller ID spoofing, and scammers don’t care whose phone number they use. One scammer recently used the phone number of an FTC employee.

Don’t rely on caller ID to verify who’s calling. It can be nearly impossible to tell whether the caller ID information is real. Here are a few tips for handling these calls:

- If you get a strange call from the government, hang up. If you want to check it out, visit the official (.gov) website for contact information. Government employees won’t call out of the blue to demand money or account information.
- Don’t give out — or confirm — your personal or financial information to someone who calls.
- Don’t wire money or send money using a reloadable card. In fact, never pay someone who calls out of the blue, even if the name or number on the caller ID looks legit.
- Feeling pressured to act immediately? Hang up. That’s a sure sign of a scam.

Want more tips for avoiding scams? Check out 10 Ways to Avoid Fraud.

If you’ve received a call from a scammer, with or without fake caller ID information, report it to the FTC and the FCC.
Criminals don’t like getting caught. So, when they want to send and receive stolen money, they get someone else to do the dirty work. Some scammers develop online relationships and ask their new sweetheart or friend to accept a deposit and transfer funds for them. Other cons recruit victims with job ads that seem like they’re for legit jobs, but they’re not. Law enforcement calls the victims ‘money mules.’ If you get involved with one of these schemes, you could lose money and personal information, and you could get into legal trouble.

Scammers post ads for imaginary job openings for payment-processing agents, finance support clerks, mystery shoppers, interns, money transfer agents or administrative assistants. They search job sites, online classifieds and social media to hunt for potential money mules. For example, if you post your resume on a job site, they might send you an email saying, 'We saw your resume online and want to hire you.' The ads often say:

- the company is outside the U.S.
- all work is done online
- you’ll get great pay for little work

If you respond, the scammer may interview you or send an online application. He does that to collect your personal information and make the job offer seem legitimate. At some point, the scammer will ask for your bank account number, or tell you to open a new account, and then send you instructions about transferring money.

If you think you’re involved with a money transfer scam:

- stop transferring money
- close your bank account
- notify your bank and the wire transfer service about the scam
- report it to the FTC
The IRS doesn’t want your iTunes cards

July 7, 2016
by
Bridget Small
Consumer Education Specialist, FTC

If anyone tells you to buy iTunes cards to pay the IRS, qualify for a grant, get a loan or bail out a family member, say “No.” They’re trying to scam you. The only place to use an iTunes card is at the iTunes store, to buy online music, apps or books.

People have told the FTC about scammers who called and demanded iTunes cards as “payment.” Bogus “IRS agents” told people they owed back taxes and would be arrested soon, unless they bought an iTunes card and gave the code to the “agent.” Phony “government grant” officers called and promised a big payout, after the person bought an iTunes card and read the code to the “grant officer.” Other fraudsters told people their grandkids were in jail and the only way to help was — you guessed it — to buy an iTunes card and read the code over the phone. All the stories were false.

There’s a reason scammers insist on getting iTunes cards: Once you tell a scammer the code from the back of an iTunes card, he takes control of the value on the card. He can use the code or sell it. After a person redeems the code, you can’t get your money back.

If you gave someone the code from an iTunes card and you think it was a scam, call Apple Support at 1-800-275-2273 right away (you may have to spend some time on hold). Tell them what happened and ask if they can disable the card. Also, go back to the store that sold you the card and talk with their customer service staff. And if you hear from someone who wants you to send an iTunes card, please tell the FTC.
Federal student tax? No such thing.
May 24, 2016
by
Andrew Johnson
Division of Consumer and Business Education, FTC

Imposters posing as IRS agents are trying to trick college students into paying a “federal student tax” – a tax that doesn’t even exist.

Students from many colleges are telling the FTC that the calls go something like this: the so-called IRS agent tells you that you owe a “federal student tax,” and often has some piece of information that makes the call seem legit. Sometimes it’s the name of your school, or another piece of information about you. The caller demands that you wire money immediately, by MoneyGram or another untraceable method. And, if you don’t act quickly enough, the caller might threaten to report you to the police. If you hang up on the caller, they might make follow-up calls with spoofed caller-ID information.

So, while caller ID might say it’s 911 or the U.S. Government calling, it’s not. It’s all fake. If you get one of these calls, what do you do? Well, first, know this: No one from the IRS will ever ask you to wire money, or pay by sending iTunes gift cards or reloadable prepaid cards. That’s a scam, every time. In fact, the IRS will never contact you by phone first. If you owe money for an actual tax, the IRS will send a letter first.

So, if you get one of these calls, hang up. Never wire money or give personal or financial information to one of these callers. Report the call to the FTC immediately. And tell your friends at school. They might get the next call!
Scams, Too
June 24, 2016
by
Lisa Lake
Consumer Education Specialist, FTC

What's worse than losing money to a scammer? Losing more money to another scammer claiming to help you recover from the first one.

Yep; this really happens. It works like this: Con artists contact you because you’re on their lists of people who lost money to scams. For a “small fee” or “donation” upfront, they promise to recover the money you lost from a prize scheme, bogus product offer, or some other scam.

Sometimes, they try to get you to contact them by putting their offers of “help” in the comments section of blog posts or online articles about scams. Some crooks claim to be from a government agency to appear trustworthy. Others pretend to be actual victims who got (supposed) help from some (fake) agency or company.

But it’s all just a scam, too — another way for a scammer to profit from your loss. They’re after your money, and if you share your payment information, they’ve got it.

Here’s how you can avoid these recovery scams:

1. **Don’t pay upfront for a promise.** Someone might ask you to pay in advance for things – like help with recovering from a scam. Consider it a no-go if they ask you for money before they provide any “help”.
2. **Don’t send money or give out personal information** in response to an unexpected text, phone call, or email.
3. **Do online searches.** Type the name or contact information into your favorite search engine with the term “complaint” or “scam.”
4. **Sign up for the FTC’s free scam alerts at ftc.gov/scams** for the latest tips and advice about scams.
   And if you find yourself scammed after being scammed, file a complaint with the FTC.
Scammers push people to pay with iTunes gift cards

May 10, 2016
by
Amy Hebert
Consumer Education Specialist, FTC

One thing we know about scammers — they want money, and they want it fast. That’s why, whatever the con they’re running, they usually ask people to pay a certain way. They want to make it easy for themselves to get the money — and nearly impossible for you to get it back.

Their latest method? iTunes gift cards. To convince you to pay, they might pretend to be with the IRS and say you’ll be arrested if you don’t pay back taxes right now. Or pose as a family member or online love interest who needs your help fast. But as soon as you put money on a card and share the code with them, the money’s gone for good.

If you’re not shopping at the iTunes store, you shouldn’t be paying with an iTunes gift card. Other payment methods scammers might ask for include Amazon gift cards, PayPal, reloadable cards like MoneyPak, Reloadit, or Vanilla, or by wiring money through services like Western Union or MoneyGram. Government offices won’t require you to use these payment methods.

If you get targeted by a scam like this, report it to the FTC at ftc.gov/complaint.