Transcript - Avoiding Online Scams Podcast

This is Carol Kando-Pineda. I'm an attorney with the Federal Trade Commission, the nation's consumer protection agency. One focus of my work is outreach to the military community, giving you tips and tools to avoid scams, watch your wallet, and protect yourself in the marketplace.

Today I'm going to talk about how to spot and avoid scams you might encounter online or in your email. Many of these scams are international. Scam artists are very clever with schemes that defraud millions of people around the globe each year. These con artists can be common crooks are part of large, criminal organizations. What do these scams look like? Here's how to spot 10 of the most common ones:

The Nigerian email scam. It's not just about Nigeria. They come from all over the world now. They claim to be officials or business people in some country and they say their money is somehow tied up for a limited time. They offer to transfer a lot of money to your bank account if you pay a fee, or taxes, or to help them access their money. If you respond you may get documents that look really official, sometimes with seals and official logos and letterhead. Then they ask you to send money to cover transaction and transfer costs and attorneys' fees as well as blank letterhead, bank account numbers, or other information. They may even encourage you to travel to the country in question or a neighboring country to complete the transaction. Sometimes they have even produced trunks of stamped or dyed money to try to verify their claims. This is very elaborate. But they vanish with your money and the harm can go way beyond your pocketbook. According to some State Department reports, people who have responded to these scams have been beaten, threatened, subject to extortion, and in some cases, murdered.

Now there are work-at-home scams. Not quite as scary, but still serious. You probably have seen the ads. They promise steady income for very minimal labor. Medical claims processing, envelope stuffing, craft assembly work, other things that maybe you could do at home. If you're part of a military family and you're moving around a lot, it makes it much harder to snag a job and these ads can be very appealing. It's fast cash, minimal amount of work, no risk. What they don't tell you is you may have to work many, many hours without pay or you'll have to pay hidden costs to place newspaper ads, make photocopies, or buy supplies and software, whatever it is that you need to do the job. So once you put in your own time and money you're likely to find that the promoters refuse to pay you, that your work isn't up to their quality standards. Let me tell you, the FTC has yet to find anyone who's gotten risk stuffing envelopes or assembling magnets at home. Legitimate work-at-home business promoters should tell you in writing exactly what's involved in the program they're selling to you. Ask questions and beware of shills that they pay to lie and sing their phony praises.

Weight loss and miracle cures have been around forever. These emails promise a revolutionary pill, patch, cream, some other product that will result in weight loss without diet or exercise. I think we all know where this is going. Some emails will tout scientific breakthroughs and miracle cures for all kinds of diseases and conditions. These are gimmicks playing on your sense of hopefulness. I mean, seriously, if there was a complete breakthrough to cure cancer or a sudden medical miracle to help people lose weight, don't you think you'd hear about it on the nightly news or in mainstream newspapers? You're not going to get it through an email.

Pay in advance credit offers. The email says you've been pre-qualified to get a low-interest loan or a credit card. Sometimes they offer to repair your credit even though banks have turned you down. But to take advantage of the offer you have to ante up a processing fee of several hundred dollars. So, what's the catch? A legitimate pre-qualified offer means you've been selected just to apply, nothing more, nothing less. You still have to complete an application and you can still be turned down. If you paid a fee in advance for the guaranteed promise of a loan or a credit card, you've been hustled.

Now, let's talk a little about debt relief. These emails say you can consolidate your bills into one monthly payment without borrowing. They'll stop creditors from harassing you, they'll stop foreclosures, repossessions, tax levies and garnishments. Sometimes they say they can completely wipe out your debts. What they don't tell you is their offers almost always involve bankruptcy proceedings. Now, bankruptcy is one way to deal with serious financial problems. It's generally considered the option of last resort, though. Why? It has a really long-term negative impact on your credit worthiness. It stays on your credit report for 10 years and can hurt your ability to get credit, a job, insurance, and even a place to live.

Then there are investment schemes. These emails tout investments that yield high rates of return with little or no risk. That's always kind of a warning sign, right? One version seeks investors to form an offshore bank, others are vague about the nature of the investment but stress the rate of return to get people very excited about it. Promoters hype their high-level financial connections. The fact that they're privy to inside information, that they'll guarantee the investment, or that they'll buy it back. That's just a way to distract you. They'll almost always try to rush you into a decision.

Alright, so now you know some of the twists and turns of these scams. Here are 10 tips, good rules of thumb to help you avoid them.

First, don't send money to someone you don't know. That includes an online merchant you've never heard of, or an online love interest who asks for money or favors. It's best to do business with sites you know and trust. If you buy items through an online auction, consider payment options that provide protection, like a credit card.

Don't send cash or use a wire transfer service. And don't pay upfront fees for the promise of a big payoff, whether it's a loan, a job, or prize money.

Second, don't respond to messages that ask for your personal or financial information, whether the message comes as an email, a phone call, a text message, or an ad. Don't click on links or call phone numbers included in the message, either. The crooks behind theses messages are usually trying to trick you into sending money and revealing your bank account information. If you get a message and you're concerned about your account status, call the number on your credit or debit card or on your statement. Check it out that way.

Third, don't play a foreign lottery. First, it's easy to be tempted by messages that boast enticing odds in a foreign lottery or messages that claim you've already won. Inevitably they'll ask you to pay taxes, fees, or customs duties to collect your prize. If you send the money you won't get it back regardless of the promises. And second, you should know it's illegal to play foreign lotteries, anyway.

Fourth, keep in mind that wiring money is like sending cash. Once it's gone, you can't get it back. Con artists often insist that people wire money, especially overseas, because it's nearly impossible to reverse the transaction or to trace the money. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or to someone who claims to be a relative in an emergency and they want to keep it secret. That's a whole other ball of wax. Just be careful. Wiring money is dangerous.

Don't agree to deposit a check from someone you don't know and then wire money back, no matter how convincing the story. This is kind of a corollary to the one we just talked about. By law, banks must make funds from deposited checks available within days but uncovering a fake check can take weeks. You're responsible for the checks you deposit, so if a check turns out to be fake, you're responsible for paying the whole amount back to the bank.

Sixth, read your bills and monthly statements regularly, whether they're on paper or online. Scammers steal account information and then run up charges and commit crimes in your name. Dishonest merchants sometimes bill you for monthly membership fees or other goods and services you didn't authorize. If you see charges you don't recognize or didn't okay, contact your bank, the card issuer or other creditor immediately.

Seven, in the wake of a natural disaster or other crisis, give to established charities rather than ones that seem to spring up overnight. Popup charities probably don't have the infrastructure to get help to the effected areas or people and they can be collecting money to finance illegal activity. Check out ftc.gov/charityfraud to learn more about that.

Eight, talk to your doctor before buying health products are signing up for medical treatments. Ask about research that supports a product's claims and possible risks or side effects. Buy prescription drugs only from licensed U.S. pharmacies. Otherwise you could end up with a product that's fake, expired, or mislabeled. It could be dangerous. Visit ftc.gov/health for more information about that.

Nine, remember, there's no such thing as a sure thing. If someone contacts you promising low-risk, high-return investment opportunities, stay away. When you hear pitches that insist you act now, or they guarantee really big profits, they promise there's no risk, especially if they want you to send cash immediately, stay away. Know where an offer is coming from and who you're dealing with. Try to find a seller's physical address, not just a P.O. box, and a phone number. With voice-over-the-Internet and other web-based technologies, it's tough to tell where someone's calling from. Do an Internet search for the company name and website, and look for negative reviews. Check them out with the Better Business Bureau – bbb.org. It's not always foolproof, but it's worth a look to see if the BBB has any complaints against the company. And you can find out an awful lot online, too, if there are complaints from other consumers.

To learn more about these scams, visit onguardonline.gov. That's the site run by the FTC and its partners in the government and technology industries. Learn more about how to stay safe and secure online and avoid Internet fraud. You can get free tips, tools, videos, and games about cyber security.

And if you've been ripped off by one of these scams, file a complaint with the FTC/complaint.

And as always, you can go to Military OneSource for help. This free 24-hour service is available to all active duty, Guard, and Reserve members (regardless of activation status) and their families. Consultants provide information and make referrals on a wide range of issues. Call 1-800-342-9647 or go to www.MilitaryOneSource.com to learn more.