Tech Topics

Easy Ways To Protect Yourself Against Phone Scams

(NAPSA)—As children, we were taught not to open the door to strangers or let an unidentified caller know our parents weren't home. Today, as adults, we've been warned not to believe an email claiming a loved one is stranded in London without money, and not to sign the back of our credit cards with anything other than "See Photo ID."

We can take precautions, but it still won't stop technically savvy criminals from trying to take advantage of consumers. Scams have become so advanced that even the most prepared could easily fall victim, with new methods surfacing too frequently. Two recent phone scams that have hit unsuspecting people with fraudulent charges are the IRS phone scam and the one-ring scam. Here's how they work:

IRS phone scam

In this particular scam, a criminal will call pretending to be an IRS agent, requesting personal information like date of birth and Social Security and bank routing numbers. Scammers prey on consumers' fear, so many people wanting to show compliance with a government agency relinquish their information to the fraudster.

One-ring scam

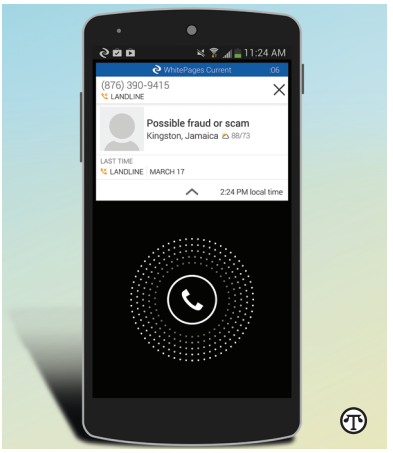
Another recent innovative scam is called one-ring, which involves scammers dialing American mobile phones from robo-calling facilities outside the United States, typically in the Caribbean, from 10-digit numbers that appear to have U.S.-based area codes. Their trick is to hang up after one ring in the hope that the recipient will be curious and call back, thinking that he or she has missed an important call. Since the number is actually international, callers are charged exorbitant connection and long-distance fees, as scammers attempt to keep victims on the line.

So how can you protect yourself?

Hang up immediately. If you get a call from a government agency or other business asking for a payment, hang up. No one from a federal government agency will ask for money over the phone, even the IRS.

Don't call a suspicious number back

In the case of the one-ring scam, the number appears like it's from the United States when it's not and, therefore, is not legitimate. Scammers are able to set up systems to ensure all incoming calls are charged—most of the time consumers are unaware of the charges.



If you get a call from a government agency asking for a payment, hang up. No one from a federal government agency will ask for money over the phone.

Use mobile apps

There are many apps that can identify callers to help ensure verification. WhitePages Current Caller ID takes call identification a step further, warning you of potential scams and providing alerts for both incoming and outgoing calls to signal users if a number is one of thousands identified as a scam.

Never provide personal information

Avoid giving out credit card information, Social Security number or other personal details to an incoming caller whom you do not know, even if you are familiar with the business they claim to represent. Some scams spoof well-known entities like Microsoft or Verizon tech support.

Do not pay money up front

If you have been contacted that you've won a contest or have been accepted for a new insurance policy, do not provide any payment. For any legitimate offer, an up-front payment is not required.

In addition to hanging up the moment a call seems suspicious, the most important rule of thumb is to never return a call to a number you do not recognize. If it is a legitimate caller, they will leave a voice mail or call back. And if you feel that you have become a victim of a scam, report the phone number to local authorities, the FTC and your mobile carrier. If you shared personal information, make sure to monitor your credit report and immediately contact your credit card company and other financial institutions.