Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

June 2024

An effort to "protect" your money may be a ruse to steal it

Some of the latest impostor scams are more complex in design and particularly painful, costing some unsuspecting consumers their life savings.

This new style of fraud often begins with a "tech support professional" claiming that one of your bank, investment or retirement accounts has been compromised – and directing you to withdraw all of your money. If you do as he or she says, the fake professional maintains, your assets will be "protected." In reality, the scammer is looking to steal every penny you've saved.

Spotting the scam early is crucial, so don't waste time – or you could sacrifice your money and personal information. The scammer is likely to express a sense of urgency, which is your clue to take a deep breath and realize that your money is safe where it is now, with a legitimate financial institution or investment professional. Following the course of action recommended by the scam artist will only mean losing your money, not protecting it.

Some advice from the Federal Trade Commission (FTC):

- Never disclose an online account-verification code to anyone who calls you, especially if the person claims to be from your bank's fraud department. Sharing a verification code will allow the scammer to "prove" he or she is you and help the scammer drain your account.

- If you receive communication from a potential impostor, stop and immediately contact your financial institution or investment professional, using contact information listed on a legitimate statement from that bank or investment company. Calling a phone number supplied by the scammer will only play into the hands of the impostor, who will answer your call and pretend to be associated with your account.

A more complex "phantom hacker" impostor scam was announced in October 2023 by the FBI in Cleveland. This scam consists of three levels of impostors:

1) **Tech-support impostor**. The scam begins with a phone call, a text message, an email or an online pop-up box directing the victim to call a phone number for "assistance." The call leads to a tech-support impostor, who directs the consumer to download software to provide the "tech specialist" remote access the consumer's electronic device. Once remote access is gained, the scammer falsely claims that the device has been hacked or is about to be hacked, then tells the consumer to check his or her financial accounts to see whether it contains any unauthorized charges. (Note: This allows the scammer to discover the specific financial institutions with which the victim has accounts.) Step 1 ends with the scammer telling the victim to expect a call from his or her financial institution's fraud department.

2) **Financial institution impostor**. A scammer impersonating an employee of the victim's financial institution calls to inform the victim that a foreign hacker has gained access to his or her account. To "protect" the account, this impostor says, all the assets must be moved to a "safe" third-party account (at the Federal Reserve, for example, or another federal agency).

3) **Federal government impostor.** A scammer pretending to represent a federal government agency "confirms" that the money in the victim's account is "unsafe" and, as such, must be moved immediately to a new "alias" account to protect it. At this point (if it hasn't already happened,), the victim might move all of his/her money to the "safe" account.

"Victims often suffer the loss of entire banking, savings, retirement and investment accounts under the guise of 'protecting' their assets," the FBI says.

The FBI provides practical tips to protect consumers from such a scam and urges victims to report phantom hacker scams to the FBI Internet Crime Complaint Center at www.ic3.gov. Remember: If you're asked to transfer money to protect your money, you're likely being scammed.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Have credit-card debt? Beware of "relief" scams

Whether the economy is robust or weak, some consumers will struggle to make ends meet or have other reasons to maintain a balance on a credit card

Legitimate debt-relief services exist, but debt-relief scammers often claim that they will help pay off a debt but instead take your money without providing any assistance.

According to the Federal Trade Commission (FTC), the following are possible signs of a debt-relief scam:

- **Upfront fees:** Scammers often want their fees upfront, before doing anything to reduce your credit-card debt. Not only is providing money upfront for this service unwise, it is also against federal law if the relief plan was offered via the telephone.
- **Unexpected calls:** A caller unexpectedly contacts you and wants personal or financial information as part of an offer to settle debts.
- **Guaranteed solutions:** Someone guarantees you a solution from a "new government program" for an extra charge or attempts to enroll you before reviewing your financial specifics.

How to lighten or eliminate credit-card debt

- **Make a budget**. Creating a personal budget can help you discover both where your income is going each month and how to reduce future spending. This FTC worksheet can help you with the process.
- **Contact your credit-card company.** Reach out to your credit-card company as soon as you fall behind on your credit-card bills. Use the call as an opportunity to explain your financial situation before a debt collector starts to call on you. You might be able to work out a payment plan with the credit-card company that you can more easily manage.
- **Seek legitimate credit counseling:** If you continue to need help, check out legitimate credit counseling options. The FTC advises consumers to look for such services "at credit unions, universities, military personal financial managers, and U.S. Cooperative Extension Service branches" – many of which charge low fees. Be sure to ask how much the organization charges, the FTC says. Another option is a nonprofit credit-counseling service through the National Foundation for Credit Counseling, which you can reach at www.nfcc.org or 800-388-2227.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515

Summer fairs, festivals, and expos: Consumer precautions and protections

For many Ohioans, summer encompasses visits to fairs, summer music festivals and gardening expositions. While enjoying such events, it's important to remain vigilant to avoid fraudsters. The Consumer Protection Section of the Ohio Attorney General's Office offers these tips for a scam-free experience:

- **Be cautious when asked for personal information.** When entering a sweepstakes, contest or drawing, be sure to carefully read the entry form, especially the small print. Companies often use entry forms as a marketing tool, and you may unknowingly consent to a sales call or the sale of your personal information to other companies, even if you're on the National Do Not Call Registry.

- **Be skeptical of "free" vacation offers.** Such offers often have strings attached, such as the requirement to buy an expensive second ticket or listening to a long sales pitch. Hidden costs and conditions may make it nearly impossible to schedule the trip. Remember: If a deal sounds too good to be true, it probably is.

- **Know your rights before signing a contract.** In Ohio, if you sign an agreement for a product or service valued at $25 or more at a fair, you can cancel the contract within three business days. This right, part of Ohio's Home Solicitation Sales Act applies to sales outside of the seller's regular place of business. The salesperson must inform you of your right to cancel and provide a form explaining how to do so.

- **Watch out for deceptive displays or misrepresentations.** Companies are required to provide all relevant information before a sale. Ensure that all promises and conditions are in writing before signing any contract.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Obituary "pirates" target personal info on deceased relatives, survivors

After losing a loved one, it's important to be cautious about the information included in the deceased person's obituary. Details about the funeral home and even surviving family members can be useful to scammers – notably obituary "pirates" who use information posted online to steal identities or perpetuate scams.

Identity thieves target obituaries because the victims are either deceased and unable to monitor financial accounts and credit reports, or emotionally vulnerable and, as such, more susceptible to manipulation.

Here's how scammers exploit obituary information:

- **Fake invoices:** Scammers may use obituary details to send fraudulent invoices from funeral homes. If they know a funeral home's name from an obituary, their fake invoices appear more convincing – and you might be more inclined to pay an invoice that accurately names the funeral home and date of service.

- **Family member scams:** Information about surviving relatives can also be exploited. If a grandfather passes away, for example, a scammer might contact the grandmother pretending to be a grandchild. Knowing the grandchild's name from the obituary makes the scam seem more legitimate. A scammer might wait months or years to act on the information, as obituaries often are archived online for an extended time.

- **Targeting the bereaved:** The mere fact that you've lost a loved one can make you a target. Scammers know you might be in a vulnerable state and potentially looking for companionship. For instance, those who have just lost a spouse may be more susceptible to romance scams, one in which the scammer pretends to have a romantic interest to steal money.

AARP notes the following red flags regarding obituary pirates:

- You receive a call from a "government official,' "debt collector" or "insurance broker" about outstanding taxes, unpaid bills or unfinished business supposedly left by a recently deceased loved one.

- The caller pressures you to pay immediately and asks for payment by wire transfer, gift card or reloadable cash card.

- After your loved one's death, you receive illegitimate bills or notice credit-card activity for purchases you didn't make.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

BONUS TIP YOU CAN USE

The Consumer Protection Section of the Ohio Attorney General's Office has published a new flyer for victims and other residents of areas affected by natural disasters. "Recovering from a Natural Disaster" can be found here.

OHIO SALES TAX HOLIDAY - GOOD NEWS TO KNOW

This year, the sales-tax holiday will span 10 days – from **Tuesday July 30** through **Thursday Aug. 8**. The event permits tax-free online and in-person purchases on all eligible items up to $500 per item. Though traditionally associated with back-to-school purchases, the holiday includes many other items. The few exceptions include boats, automobiles, liquor, tobacco, vapor products and items containing marijuana.

When shopping, make sure that you understand which items are eligible for the exemption. Also, practice sound shopping habits, such as keeping receipts and knowing the return policies of the stores where you shop.

The Ohio Department of Taxation provides detailed information about the expanded sales-tax holiday. Before heading out, consider the types of purchases you plan to make and review the Department of Taxation's FAQs to understand the exempted items.