Ohio Attorney General's
Consumer Advocate
Newsletter
AUGUST 2013

Unexpected Email: Think Before You Link

If you've ever received a vague email urging you to provide personal information or click on a link within the message, you're certainly not alone. Maybe the email advertised an amazing sale or great job opportunity and made you curious to learn more. Before you click, remember that it's important to weigh the potential for succumbing to a scam.

Since the beginning of the year, the Ohio Attorney General's Office has received more than 90 complaints involving unsolicited emails. Some emails prompt recipients to click on a link to collect "unclaimed funds from the government." Others claim the recipient has been selected for a work-at-home opportunity as a "survey taker" or "mystery shopper." However, the recipient must reply with personal information to be considered.

Regardless of the pitch, the result is the same. These emails are designed to trick you into revealing personal information. Clicking on their seemingly harmless links or attachments may download malicious software to your computer, including viruses designed to scan for Social Security numbers and banking information. These viruses may increase your risk for identity theft.

To deal with potential scam emails:

- Copy and paste the first few sentences or first paragraph into an Internet search engine and add the word "scam." The results may indicate whether others have received and reported similar emails.
- A scam email may look very similar to one from a legitimate business, so be very careful about clicking any links, including an "unsubscribe" button at the bottom. Clicking the link may download a virus rather than remove your email from the list.
- Designate unwanted email as junk prior to deleting it so future email from that sender is routed to your junk mailbox.
- Limit unwanted emails by not signing up for free giveaways or surveys. Often, companies sell your personal information to other companies — and possibly scammers.
- Skim the email for misspelled words or grammatical errors. Since email scams sometimes originate outside the United States, errors could signal a scam.
- Be wary of emails requesting money. Even if the message appears to be from a friend or family member in need of urgent help, think twice before responding or sending money. The message could be a sign that your friend's email account has been hacked. Also, be leery of emails that only contain a link to a website; this commonly happens when email accounts are hacked.

If you suspect a scam or an unfair business practice, report it to the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

Be Wary of Back-to-School Scams

The back-to-school season can be a busy time for families. Unfortunately, scammers are busy this time of year, too.

Carefully evaluate back-to-school offers. Here are some pitfalls to avoid:

- Scholarship or grant scams: Be wary if someone asks you for advance fees in exchange for helping to find or obtain scholarships or grants. You usually can find scholarship information online for little or no cost. If a scholarship is legitimate, it shouldn't require an advance fee. The government will not ask for processing fees for grants you have already been awarded. If you are looking for grants for higher education, these are awarded through each school's financial aid office after potential recipients fill out the Free Application for Federal Student Aid (FAFSA) at www.fafsa.gov.
- Identity theft: Providing information to receive financial aid may make you vulnerable to identity theft. Make sure you are applying through the proper site, www.fafsa.gov. Don't provide personal information over the Internet or phone unless you initiate the process. Services that ask for personal information and a fee to file for financial aid may sell your personal information or use it improperly. To avoid becoming a victim of identity theft, review financial aid statements and keep track of amounts owed. View your credit report for free at www.annualcreditreport.com to see what accounts are associated with your name. You can do this for free three times a year — once through each of the three major credit reporting agencies.
- Job scams: If you want to make extra money while you're in school, keep in mind that some job postings are fraudulent. Never pay someone in order to get a job, and beware of online ads that promise great earning potential but offer little concrete information about the work. Don't trust potential employers who say they're out of the country and will pay you to process funds or run errands for them. Also be skeptical of offers for "mystery shopper" positions. These are often scams.

If you've been a victim of an unfair practice or scam, file a complaint with the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

Also, check out the Attorney General's tips for evaluating advertisements and knowing your rights.

Take a Good Look at Your Phone Bill

Your phone bill may just be another one on the list to pay every month. But next time it arrives, take a second look for extra charges or fees. Some may be for services you didn't order, agree to, or use. If you find these, you may be a victim of "cramming."

Cramming occurs when third-party companies, not your phone company, add charges to your phone bill. They may be nominal amounts, such as $2 to $3, which you might not catch at first glance. Larger cramming charges may be for services that sound legitimate such as "web hosting" or "member fees." Since these charges come in various amounts with many different names, they can be hard to identify.

The best way to avoid cramming charges is to review your phone bill closely every month. Once you become familiar with various charges, cramming will be easier to spot. Watch for charges that have generic-sounding names, and look for numbers with unfamiliar area codes. Cramming charges may include:

- Subscriptions for Internet-related services, such as web hosting
- Access to restricted websites
- Entertainment services with a 900 area code
- Collect calls
- Club memberships

Sometimes you can't do anything to stop a determined crammer from filling your phone bill with unauthorized charges. But you can avoid some of the common ways crammers get your number. Avoid the lure of "free" offers, whether entering a contest, joining a club, or getting extra phone minutes. You may be giving permission to the company to enroll you in a service and never receive the promised item.

If you see an unfamiliar charge on your phone bill, call your phone company and ask for an explanation. Consider requesting that your phone company block all third-party charges.
To report cramming or an unfair or deceptive business practice, contact the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

Beware of Scams when Buying or Selling Online

Online marketplaces make it easy for buyers to access countless products from individual sellers. But shopping this way can leave you vulnerable to scams since you may not know who is selling the item or if the item even exists. Scam artists take advantage of these unknown elements and attempt to steal your money.

Fake listings are a common ploy to deceive buyers. Listings may have been copied from another source or not exist at all. Purchasers don't receive the item, and they're also out their money.

For example, an Ohio consumer saw a truck advertised through an online marketplace. He contacted the "seller" and received a link, supposedly to an escrow service that would hold his payment until the vehicle was shipped. The escrow service was offered by what appeared to be a legitimate company. A "company representative" contacted the consumer to assist with the payment, and the consumer provided bank account information for a wire transfer. The truck never arrived, and the "seller" and "representative" disappeared. After calling a company reportedly associated with the escrow service, the consumer discovered the business does not even provide such services. In the end, this scam cost the consumer $7,800. He was out the money he wired, and he received no new wheels in the deal.

Scammers also target individuals selling items through online marketplaces. If you're a seller, watch for an overpayment scam intended to steal your money and the item you are selling. These typically happen when a scam artist sends a check for an amount greater than the asking price and asks the seller to wire back the difference, keeping the purchase amount. The check appears to be legitimate, but after a few days it bounces and any money wired to the "buyer" is lost along with the item sent.

If you are buying or selling products through an online marketplace, follow these tips to avoid scams:
- Be skeptical of sellers who ask you to wire transfer money.
- Tailor searches to local areas and deal with individuals in your area.
- Meet in a public place to exchange payment for the product.

- Research the reputation of the person with whom you are doing business, if possible. Check the seller's online rating, and do an Internet search to find any additional information about the seller.
- If possible, conduct cash transactions.
- Be wary when sellers want to use an escrow service to "guarantee" the transaction.
- Only make payments on secure websites, which begin with "https" rather than "http."
- Read and heed the fraud warnings that online marketplace websites provide.

If you've been targeted in a scam, file a complaint with the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.