Mass Consumer Affairs Blog (/collections/mass-consumer-affairs-blog)

BLOG POST

# Tips to Protect Yourself From Phishing Scams

Notices & Alerts

**OCABR and HIC December Move Update!** | *Updated Dec. 5, 2024, 07:41 am*

Starting December 14, any mail for the Office of Consumer Affairs and Business Regulation, including HIC and Lemon Law Programs, should be sent to 1 Federal Street, Suite 0720, Boston MA 02110-2012.

Contractors: There will be NO in-person HIC registration service from December 16 – January 6. For hands-on help with registration, call our Consumer Hotline, Monday-Friday, at 617-973-8787, 9 a.m.-4:30 p.m.

Contractors: From January 7–March 25, HIC in-person registration service will be on Tuesdays, by appointment only. To make an appointment, or for hands-on help with registration, call our Consumer Hotline, Monday-Friday, at 617-973-8787, 9 a.m.-4:30 p.m.

4/01/2022


As technology continues to advance, identity thieves are also becoming more clever. Scammers are constantly developing new, nearly undetected, tactics to trick their targets.  The most common way consumers are defrauded online is through phishing.  The Federal Bureau of Investigation's Internet Crime Complaint Center recorded over twice as many incidents of phishing than any other type of cyber-crime in 2020.

## What is phishing?

Phishing is when a scammer sends a fraudulent email pretending to be a legitimate entity in an attempt to access the recipient's personal identifying information.  Once a fraudster obtains these private details, which can be anything from account passwords to Social Security numbers or credit card information, he or she will try various methods to access online accounts and finances.

The most common phishing attack happens via email, but there are different techniques scammers may use depending on their target. Some phishing efforts can occur by phone calls or text messages, these types of scams are called vishing (voice phishing), or smishing (SMS phishing).  The term "whaling" is used when the target of a phishing campaign is an organization's president or senior executive. No matter what the type of phishing, the main goal of this type of fraud is always to convince an individual to provide sensitive information that will later be used illegally.

## How to spot a phishing scam:

The most successful phishing emails are carefully constructed to look identical to messages received by well-known companies or senders. These messages are often difficult to distinguish from real emails. Keep an eye out for these red flags when scanning your inbox for phishing scams:

- **Attractive, "To-Good-To-Be-True" Offers:** If an email is promising you something too good to be true, it probably is. These attractive offers are designed to immediately grab your attention and detract from other details within the message. If you are offered a large sum of money, a new phone, vacation, car, or other prizes, verify the sender or just ignore the message.
- **False Sense of Urgency:** If an email demands that you act quickly, or presents a limited-time opportunity that failure to claim will result in a severe, negative action, take your time to read and understand the message. A reputable organization, including government entities, will not contact you via email threatening a consequence if you do not comply with the message guidelines. Call the sender's business directly to discuss the email message using a verifiable phone number, never reply to these emails or use the contact information within the message.
- **Fake Hyperlinks:** If an email looks suspicious, ensure that any websites or links provided are going to a safe website. Or skip clicking on email links completely and visit the entity's website you are familiar with. A common tactic used by phishing scammers is link manipulation where a malicious hyperlink is inserted to look like it belongs to the organization sending the email. Often these fake URLs will be misspelled to deceive you. Other times, the fake link will be disguised as a text box, asking you to "Click Here." Make sure to hover over the text box to view the actual web address.
- **Corrupt Attachments:** If you received an attachment from a questionable email, do not open it without first confirming the documents with the sender. Similar to hyperlinks, attachments in phishing emails usually contain malicious viruses or ransomware.

## Avoid phishing scams:

While scam tactics and technology are always updating, there are some simple proactive steps you can take to stay safe from phishing. Consider these steps to help you spot phishing attempts:

- Add spam filters to your email.
- Never email personal or financial information without proper security protocols.
- Do not respond to messages seeking personal information via email.
- Call the sender directly to verify if a message you received is legitimate.
- Check that the website you are visiting is secure. Look for a lock icon or an address that begins with "https:" indicating that the site is secure.

If you have reason to believe you are involved in a phishing scam, the Office of Consumer Affairs and Business Regulation (OCABR) has **resources to help victims of identity theft** (/service-details/identity-theft). For more information or resources related to scams and identity theft, you may contact the OCABR Consumer Hotline at 617-973-8787, Monday through Friday between the hours of 9:00 am and 4:30 pm.

## Office of Consumer Affairs and Business Regulation

The Office of Consumer Affairs and Business Regulation protects and empowers consumers through advocacy and education, and ensures a fair playing field for the Massachusetts businesses its agencies regulate.