

Phil Archer

The Monthly Brief

Volume 10 Issue 8

August 2022

TOP 10 PHISHING LURES

Scammers are getting better at spoofing companies used in their phishing attacks. They hope that by impersonating well known companies, you're more likely to click on a malicious link or attachment to install malware or steal your personal info.

Scammers can use any company from the largest like Amazon, right down to your local utility company to appear legitimate.

Lately scams targeting those seeking a new job or career have become popular and since LinkedIn is a leading site to find work, it's now the #1 company scammers spoof in phishing emails worldwide.

According to Check Point Research, the LinkedIn business platform is impersonated in nearly half of all global phishing attacks.

Emails such as "You appeared in 8 searches this week" or "You have one new message" can be authentic, but you need to verify the sender's email address to ensure it's really from LinkedIn.

Here's the CPR top ten break down:

LinkedIn (45%), Microsoft (13%), DHL (12%), Amazon (9%), Apple (3%), Adidas (2%), followed by Google, Netflix, Adobe, and HSBC all at (1%).

You can avoid becoming a victim by following these and other great prevention tips from the [Federal Trade Commission](#).


Maintain Security Software; Use 2 Factor Authentication; Never follow or click links in unsolicited emails/text messages; Inspect URL's and email addresses for additional letters, numbers, or misspellings.

*komando, CheckPoint, FTC

Follow Us On Facebook

Subscribe: philarcher@sa18.org


Hurricane Hustlers

 In addition to preparing for the effects of a hurricane, Floridians should also be on the lookout for scammers posing as contractors offering to clean up debris and repair damage after the storm. Calling them "fly-by-night opportunists," the [BBB says storm chasers](#) tend to arrive in disaster areas after the weather has passed, seeking to scam unsuspecting victims in a vulnerable moment. In addition to the outright crooks, some out of area unlicensed contractors will also attempt to pose as a locally known company. Regardless the idea is to take advantage of your desire to get your home fixed quickly. Then take your money and do little, none, or shoddy unpermitted work.

Here are a few red flags to watchout for: Door to door workers claiming to have leftover materials from another job and can save you money. An unsolicited contractor who shows up claiming your home has serious structural or unidentified roof damage. Salespeople using high pressure tactics to get quick decisions and a signed contract before you can check them out. Contractors who want full or a majority of the repair cost paid in advance. Anyone asking for payment in cash or through a payment app. Always consider using your credit card for deposits as it can provide you with some protection. Companies without a local address, a verified Florida contracting license, or using unmarked or out-of-state registered vehicles. Learn more about these scams and protecting yourself from the [Florida Attorney General](#), and this informative article in the [Mitchell Republic](#).

*BBB, FL AG, MitchelRepublic

CAR BUYING SCAMS

 Used cars are in high demand, and scammers know it. Con artists are using online platforms like Craigslist, Facebook Marketplace, eBay, and others to list popular cars at very low prices. When a buyer contacts them, the car is located out of the area and some hardship has forced the sale. But the seller has a transport company who will deliver it at the stated price, just pay the transporter who will hold the funds in escrow till its delivered. Some even send links to 3rd party escrow companies that seem realistic but aren't.

Once you've paid the third-party company, usually by a wire transfer or prepaid debit card, your vehicle won't be delivered. The sale was a scam, and the con artist was in cahoots with the third-party company. Unfortunately, your money is gone for good.

An [in-depth investigative study](#) by Better Business Bureau (BBB) finds that thousands of consumers have fallen victim to this scam, with losses totaling millions of dollars. Red flags include prices well below market value, avoiding speaking by phone, giving vague answers, won't confirm the vehicle location for inspection, or claims another buyer is waiting if you don't want the car right now. Always have a car inspected before buying and never wire funds. They are hard to track and no way to get your money back.

For more information on vehicle shipping and escrow scams read the [BBB report](#), tips from [Craigslist](#), [Facebook Marketplace](#), and [eBay](#). If you've been scammed contact law enforcement first. Then follow-up with reports to the [FTC](#), [FBI](#), your [local BBB office](#).

*BBB, Craigslist, Facebook, FTC, FBI, eBay.