Amazon Customer Support Scams

CONSUMER ADVISORY

Scammers are pretending to be Amazon workers and contacting people claiming there's a problem with their accounts or orders. Why? To steal personal and financial information, extract money from you or to gain access to your computer.

WHAT WE ARE SEEING

More and more people and businesses are receiving calls and notifications from individuals claiming to be with Amazon customer support or Amazon security services. Use caution and don't be fooled by phone calls about problems with your Amazon account; these communications are typically not what they seem.

The current pandemic has been a catalyst for surging online sales and deliveries. We also are experiencing the 2020 Holiday Season. Our purchase behaviors, selections, and frequency of orders are very different than previous years. Many households are receiving multiple online deliveries each week. So why would a phone message or email from Amazon seem so unusual? After all, Amazon is huge corporation, used by a large segment of the population, and carries a widely known and well-established brand. Much like government imposter calls, these solicitations may appear credible on the surface.

Typical Messaging

The consumer receives a call or message from someone claiming to be with Amazon customer service indicating that some degree of suspicious activity has been documented on their Amazon account. Messages are being received through phone calls and messages, emails, texts, and even through Messenger (Facebook).

Messages and Activities May Involve:

- Potential security breach
- Fraudulent charge(s)
- Unfulfilled order
- Lost package
- Order confirmation
- "Your Amazon Account Is Locked - Order Is On Hold"

Red Flags - Instructions Given by Scammers

- Message leaves a callback number. Do not trust a phone number provided in a message as the number is fake and not tied to Amazon. Numbers are often spoofed.
- An email or text is sent, which provides a fraudulent number to call or provides a website link to a phony Amazon website.
- If the consumer responds, scammers will then ask for a login and password, credit card information or may request remote access to the consumer's computer to solve the fake problem.
- The scammer may tell the consumer to go to unusual sites, enter codes or other information, make odd purchases or charge a fee.
- If computer access is gained, the scammer can potentially access bank accounts, passwords, and other sensitive information, as well as install malware.

NEGATIVE CONSEQUENCES

Regardless messaging method, the ultimate motive is to obtain the consumer's personal and financial information. Scammers have been successful in obtaining social security numbers, sensitive banking information, driver's license numbers, credit card information, tax IDs, and other personal information.

AMAZON SAYS

According to the REAL Amazon

"Amazon will never send you an unsolicited message that asks you to provide sensitive personal information like your Social Security number, tax ID, bank account number, credit card information, ID questions like your mother's maiden name or your password."

Amazon states that the company will occasionally call its customers, but the company *"will never ask for personal information in emails, text messages, or calls. Amazon will never ask you to make a payment outside of our website and will never ask you for remote access to your device."*

Beware - Look Out For

- Attachments or prompts to install software on your device.
- Typos or grammatical errors.
- Forged email addresses to make it look like the email is coming from Amazon.com.

When in doubt, go directly to Amazon or the Seller Central website!

*If You Receive the Following, Go To **YOUR ORDERS** To Verify:*

- An order confirmation for an item you didn't purchase or an attachment to an order confirmation.
  (Is there an order that matches the correspondence?)
- Requests to update payment information that are not linked to an Amazon order you placed or an Amazon service you subscribed to.
  (If you aren't prompted to update your payment method on that screen, the message isn't from Amazon.)

Visit Amazon Website For Legitimate Communications: Click Here
Visit Amazon Website For Fraud Tips: Click Here

REPORT FRAUD

- Report Suspicious Emails and Websites to Amazon: stop-spoofing@amazon.com
- Report Phone Calls, Text Messages, Emails to Federal Trade Commission (FTC): www.ftc.gov/complaint
- Reach out to the DA18 Consumer Fraud Protection Hotline for questions and assistance.

Contact Consumer Fraud Protection
18th Judicial District
Hotline (720) 874-8547 | consumer@da18.state.co.us