With so many people shopping online, package deliveries are on the rise… doubling since 2010. Scammers, never missing a beat, are taking advantage of this to fool consumers into giving out their personal information.

The Oakland Police Department would like to remind residents to remain vigilant when shopping online and to always safeguard personal information including credit card numbers, social security numbers, PIN numbers and passwords.

It is easy to fall victim to some of these recent scams if you are not careful, scammers are pulling out all of their best tricks to gain access to your accounts.

Here are some examples:

**How the Scam Works**

You receive a call or an email from someone claiming to be your mail carrier or a parcel delivery service saying that they were unable to deliver a package to your home. If you don’t remember ordering anything that needs to be delivered, the caller may try to convince you the package is a gift from a friend or relative. The caller may sound friendly and professional, making the scam harder to spot. The email messages also look legitimate - containing official logos and using professional language.

However, things get suspicious quickly. The caller will ask you to verify personal information or give them your credit card information to reschedule the delivery. Email messages may ask you to click on a tracking link for your mystery package. When you click, you may download malware onto your computer that gives con artists access to any personal information and passwords. No matter the method of contact, the package doesn’t exist. Sharing your personal information puts you at risk for identity theft.

**How to Avoid Package Delivery Scams**

* **Be wary of unsolicited communications.** Package delivery companies will never contact you unsolicited via telephone call. Instead, if a package cannot be delivered, they usually will leave a note on your door. They may follow up with an email, but most official communications will be within your secure online account.
* **Track your packages.** Always keep track of your online purchases and expected deliveries. Request tracking numbers so you will know when each
* package is due to arrive. When you know what you are expecting, it will be harder for a scammer to fool you with the claim of a fake package delivery.
* **Never give your personal information to strangers**. Even when the caller is friendly, always use caution when asked for personal information. You can always hang up, look up the official customer service number, and directly contact the company to confirm their request. Whenever possible, use the customer service contact information or chat function within your account at the company.
* **Never click on links in unsolicited emails**. Links in emails can download malware onto your computer. Don’t click links in emails from people you don’t know or from companies who you have not asked to be contacted by. Be wary of official-looking email; popular brands can easily be spoofed.

**Another example: The “Verizon Wireless” scam:**

**How it works:**

[Scammer]: Hello Sir, I’m calling from Verizon Wireless to alert you to an order on your account that we believe wasn’t made by you. We’ve put a security restriction on your account but want to make you aware. There was an order for an iPad made to New York, while we have your billing address as *[YOUR ACTUAL ADDRESS]* which doesn’t match the order. We wanted to make sure you were aware of this order in case someone has taken control of your account.

[You]: No, I certainly did not make any orders for a new iPad on my account.

[Scammer]: Thank you, we’ll put a stop to the order and will set a security *lock* on your account. First I need to verify who I’m speaking with so I will send you a PIN code via text message and I need you to read that back to me.

[You]: Okay

[Scammer]: Okay I have sent the PIN code, please read it back to me.

Once the scammer obtains your PIN code, they are now able to reset your Verizon Wireless password and make purchases on your account.

***A better option would be***…

[You]: No, I don’t feel comfortable with this. I’m not going to read the PIN back to you.

[Scammer]: Okay, I do encourage you to act on this as soon as possible to secure your account and thank you for being a Verizon customer.

*Hang up.*

There are a few things that may appear to validate the incident to you. To start, the number they call from, which is being spoofed, may be the actual Verizon support number. You see in the text message (that actually came from Verizon) that the number matches up. The second part is just a common tactic that is used in order to break into accounts and order phones/SIM cards etc., and ship them elsewhere. Lastly, the scammer knows your actual billing address and provided it to you as evidence during the call.

However, think about it…why would Verizon need to send ***you*** a password reset code and have ***you*** read it back to them?

The scammer was using the password reset tool on Verizon and once he/she obtained the code from you, they were able to change your password to anything they wanted.

**Stay vigilant at all times:**

It’s always a wake-up call when a scam gets this close to you, they are using all of the tricks possible. This scammer may even stay ‘in character’ all the way to the end after you deny them access.

The best process to follow is to hang up and call back on the actual support number. Use the company’s website and go to their support center and get the official phone number or email address. Even with the best computer security you can have, if you open the ‘front door’ for scammers and let them into your accounts, your computers, etc. you put your personal information at risk.

Often times **you** are the first line of defense, so stay sharp out there and please feel free to reach out to us with any questions you may have. We are here to help!

The Oakland Police Department: 201-337-6171