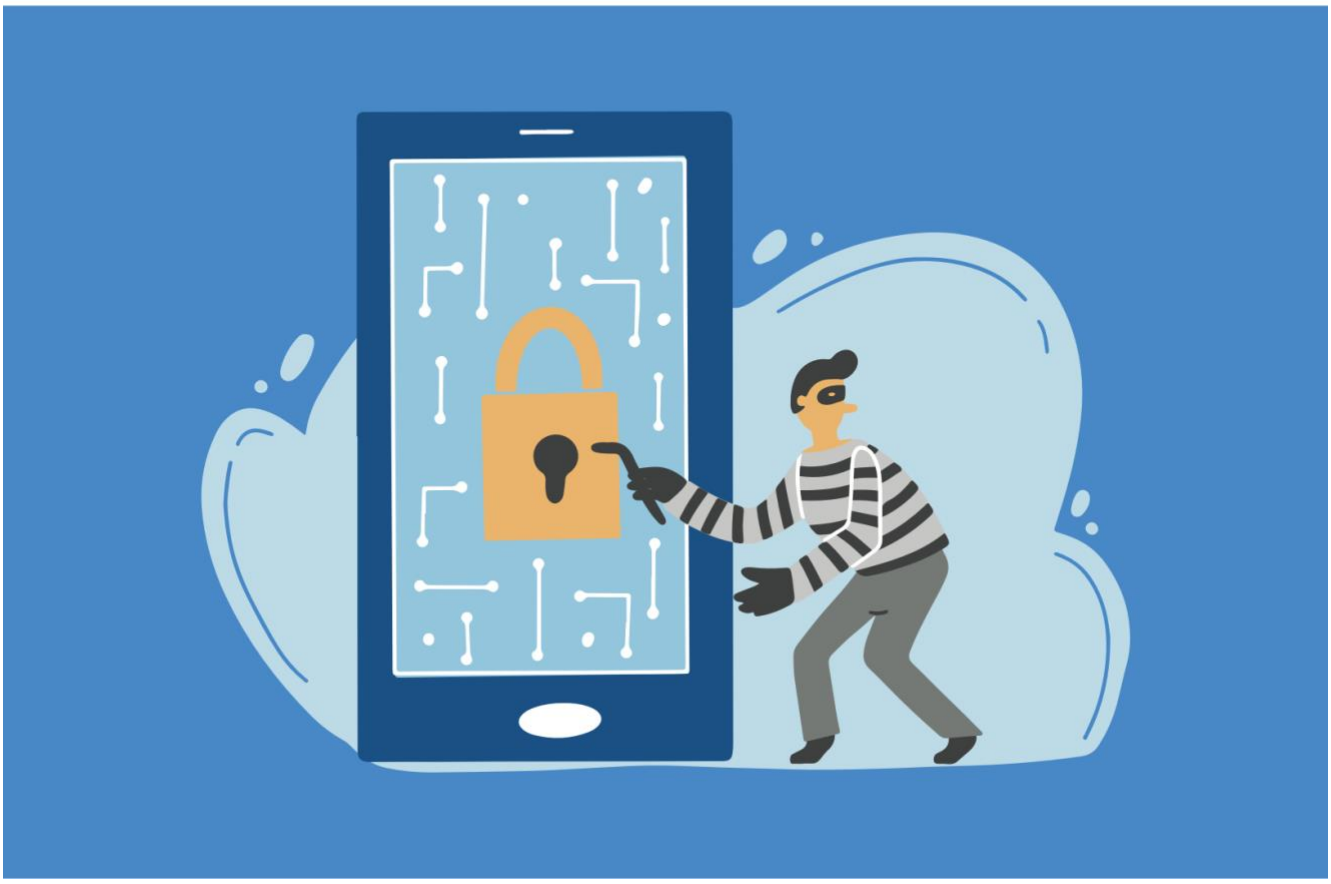
ISLAND FEDERAL BLOG



Financial Security: Beware of the New Pending Package Scam!

Everyone loves a surprise package, and scammers are taking the excitement out of that experience by using bogus packages as a cover for a nefarious scam that tricks victims into sharing their personal information — and their money.

Here's all you need to know about the pending package text scam:

How the scam plays out

In the circulating package delivery scam, the victim receives a text message from a contact who is an alleged mail carrier, or someone representing a package-delivery service. The contact tells the victim they were unable to deliver a package to the victim's home. The message might claim the package is a gift from a friend or relative and may be worded professionally, making the scam difficult to spot.

The victim is asked to reply to the message to confirm their identity; however, as soon as they engage with the scammer, they will be asked to share their personal information or credit card details to schedule delivery. This, of course, places the victim at risk for identity theft.

In other variations of the scam, the victim is contacted by email or phone. In each scenario, the scam plays out in a similar manner, with the victim convinced there's a package waiting for them, and willingly sharing sensitive data with a criminal.

Some scammers take the ruse a step further by sending the victim a text message or an email containing an embedded link. The victim is instructed to click on the "tracking link" to track the package or change their delivery preferences. Unfortunately, clicking on the link will download malware into the victim's device. Alternatively, the link connects the victim to a form asking for their personal information, which the victim often shares willingly.

Red flags

There are two primary red flags that can serve to warn you about the pending package scam.

First, the original text, email or phone call, will generally not inform the victim of the identity of the company they represent. The scammer will only claim to be an employee of a mail or package delivery service, but will not verify if they work for UPS, FedEx or another legitimate organization.

Second, the scammers don't always check if the victim actually has a package in transit. They'll either assume the victim has recently ordered something online or they'll claim a friend or family has sent a surprise gift. If you know that neither of these is true, you can be on the alert for a possible scam.

Don't get scammed!

Take these precautions to avoid being the next victim of a pending package scam:

- Be wary of unsolicited communications. Your mail carrier and package-delivery services will never contact you via text message or phone call. If a package cannot be delivered for any reason, they will usually leave you a note on the door.
- Be wary of "professional" emails sent from unsecure addresses. Any online communications from the USPS or a mail delivery agency will be sent via their own secure domain. Always be suspicious of emails sent from unsecure addresses.
- Track all incoming packages. After placing an order for an item, record the tracking number for the package so you can easily verify its whereabouts. This way, you can quickly confirm the authenticity of any suspicious texts, emails or phone calls about your package.
- Never share personal information with an unverified contact. Be super-wary when asked to share sensitive information via text, or when online or on a phone call. If you suspect fraud, end the conversation immediately and do not engage further.
- Never click on links in unsolicited emails. Links in emails can download malware onto your computer or device. Don't click links in emails from people you don't know or from companies you have not asked to contact you. Be wary of official-looking email; popular brands can easily be spoofed.

If you've been targeted

If you believe you've been targeted by a pending package scam, it's important not to engage with the scammer. Delete any suspicious text messages and block the number of the contact. Similarly, delete suspicious emails and mark them as spam. You can also report the scam to the local authorities and to the Federal Trade Commission. Finally, it's a good idea to warn your friends and family members about the circulating scam