

Incentives and threats: How to avoid scammers 'phishing' for money, personal information

March 2 2023, by Gita Sitaramiah



Credit: Pixabay/CC0 Public Domain

There are certain rites of passage in life. Milestone birthdays, graduations, marriages or births. And of course, that first email from a Nigerian prince who wants your bank account number to safeguard money with the promise you'll receive a fortune in return.

That long-running con is one of many scams plaguing U.S. consumers today in an onslaught that can feel relentless, with criminals targeting you by mail, email, phone, text and even social media.

"Scammers are always trying new ways and old ways to take advantage of us, and especially our [emotional states](#), to do two things: to steal our [money](#) or take our identity," said Bao Vang, a spokeswoman for the Better Business Bureau of Minnesota and North Dakota.

Now, scammers are even going after consumers at their jobs, posing as executives on vacation using personal email accounts to have an invoice paid, only for the payment to end up in the scam artist's pocket.

"When these spear-phishing emails come, the people are much more likely to disclose invoice data, confidential data, because it's coming from a trusted name," said Tami Hudson, a Wells Fargo cybersecurity client officer.

Your instinct may be to assist a higher-up as soon as possible, but first verify internally the request is legitimate.

If more people had the tools to understand how scams operate, they could avoid being a victim, Vang said.

First, you don't need to understand all of the scams. "In fact, that would be overwhelming," said Jason Zirkle, training director for the Association of Certified Fraud Examiners. "You just need to know they are going to ask for money or information."

The pressure tactics for you to share information or money can come either as a carrot or a stick. "The two hallmarks on the front end is they are either trying to offer you some kind of positive stimulus or threaten you with negative stimulus," Zirkle said.

For instance, be wary if a potential online love interest starts asking for money or [gift cards](#) or someone claiming to be an IRS agent contacts you and demands immediate payment.

Some of the more common types of scams consumers report to the Better Business Bureau include:

- Online purchases where what you paid for isn't what arrives on your doorstep, if it arrives at all. Hint: Legitimate online stores should provide you with a physical address and working phone number in the contact section. Vang also suggests using [credit cards](#) to pay, which have more protections than debit cards. Setting up automatic payment notifications to monitor your accounts will also help you keep track of potential errant charges.
- Phishing calls, emails and texts that look real but aim to obtain cash or personal information. Don't reply, even if [scam](#) artists call you from a "spoofed" [phone number](#) that appears on CallerID as a legitimate bank or institution. Never feel pressured to give out Social Security numbers or make payments on the phone, and don't allow remote access to your computer.
- Employment offers, often for online and social media work, that are phony. Look for a professional website, legitimate contact information and public reviews. Keep in mind no legitimate company will ask you to pay them to get a job, according to the BBB.
- Lottery and sweepstakes where you're told you've won a prize but have to send money in first to receive it. Never send money to receive money, a common tactic across many scams including the notorious Nigerian prince scheme.

Stay calm and keep these tips in mind. So when that next text message promising a free iPhone 14 or email offering a large cash sum from some foreign dignitary pops up, you'll know what to do and, most

importantly, what not to do.

2023 StarTribune.

Distributed by Tribune Content Agency, LLC.

Citation: Incentives and threats: How to avoid scammers 'phishing' for money, personal information (2023, March 2) retrieved 25 April 2024 from <https://techxplore.com/news/2023-03-incentives-threats-scammers-phishing-money.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.