## Plumas Bank presents:

# *Don't take the bait!*

A few letters can make all the difference.

Case in point: Fishing (with an "f") is awesome and often involves a restful afternoon at a lake and maybe a meal if you're lucky. Phishing (with a "ph"), however, is not awesome and often involves stress, compromised personal data — and worst-case scenario, the loss of your hard-earned money.

October is National Cybersecurity Awareness Month, so Plumas Bank is sharing a cautionary tale about one of the most common cybersecurity threats to individuals and small businesses: phishing.

### *Reeling You In*

In general terms, phishing is how bad actors fraudulently use electronic means like e-mail and texts as lures, attempting to hook the "fish" (that's you) for passwords and financial data.

The goal is to get you to take some sort of action in response to a phone call, voicemail, text or other communication. These messages often:

- Create a false sense of urgency — someone is asking you to do something right away.
- Request sensitive information, like your logon credentials, a password or account number.
- Include unexpected links or attachments.


According to Sarena Barker, Plumas Bank Senior Vice President and Digital Banking Manager, "Phishing schemes usually culminate in asking you to do something — like open an attachment, click a link, or divulge personal details — often accompanied by a scary message about what happens if you don't do so immediately."

### *Leaving the Bait Behind*

So how can you avoid being hooked? Barker says messages must be received with a heightened sense of distrust.

"As sad as it is, you must assume that messages or emails that request you to click a link, open an attachment, or provide sensitive information are a phishing attempt," she says. "Never open an attachment or click a link unless you are 100 percent sure of its legitimacy."

A few other tips:

- Beware of websites that look real but have typos or are missing the "https" in the address bar.
- Make sure your software and browsers are up to date, as security patches are constantly released in response to the loopholes that phishers discover and exploit.
- Keep in mind that no company will ever call you asking for your logon credentials to a website. (It's a different story when you call them, as they may ask for account numbers or a password you've created for them to verify your identity.)

### *Hooked? Here's What to Do Next*

But mistakes happen, and occasionally, the bait is taken. First and foremost, Barker advises, don't feel embarrassed. Bad actors are increasingly sophisticated in their approaches, so it can be easy to fall prey to a phishing expedition.

"If you accidentally click a link or supply some information that you now feel suspicious about, notify someone immediately — like the legitimate source where the communication was allegedly from," she recommends.

To learn more about steps you can take to keep yourself and your money safe, explore tips at plumasbank.com/cybersecurity.

***Learn more at plumasbank.com.***

PLUMAS BANK
HERE. For Good.
Member FDIC