Tips to avoid

Phishing Scams

include:

Verify the Source:
Always double-check the sender's email address or phone number. Scammers often use addresses or numbers that look similar to legitimate ones.

Be Cautious with Links:
Hover over links before clicking to see the actual URL. If the URL looks suspicious, **do not click!**

Do Not Share Sensitive Information:
Legitimate organizations will never ask for a password, Social Security number or credit card details via email or text.

Gift Cards = Red Flag:
Anytime a message is requesting a consumer to send a gift card as payment, it is more than likely a scam and communication with the entity should be terminated immediately.

Use Multi-Factor Authentication:
Enable this added security layer onto all accounts to prevent an information breach.

Keep Software Updated:
Regularly update operating systems, browsers and software to protect against the latest threats.

Florida Attorney General's Office Scams at a Glance:

One Phish, Two Phish

Phishing scams should be reported to the FBI's Internet Crime Complaint Center at IC3.gov

Visit MyFloridaLegal.com to find consumer tips or to file a complaint.

Report fraud by calling
1-866-9-NO-SCAM
(1-866-966-7226)

View other Scams at a Glance resources at:
MyFloridaLegal.com/ScamsAtAGlance

Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399-1050

03/2025

MyFloridaLegal.com

Scams at a Glance:

One Phish, Two Phish

OFFICE OF ATTORNEY GENERAL

JAMES UTHMEIER

SAFE ★ STRONG ★ FREE

SCAM ALERT

What are Phishing Scams?

Phishing scams are fraudulent attempts by cybercriminals to obtain sensitive information such as usernames, passwords and financial details by disguising themselves as trustworthy entities. These scams often occur through email, text messages or phone calls, where the scammer impersonates a reputable organization or individual.

How Prevalent are Phishing Scams?

Phishing is the most common form of cybercrime, with an estimated 3.4 billion spam emails sent every day. Reports show that more than 83% of companies experience phishing attacks. The rise in remote work and increased online activity is only amplifying the opportunities for these scams.

Examples of *Phishing Scams*

Email Phishing

An email appears to be from a bank, asking a consumer to update account information through a provided link. The link leads to a fake website designed to mimic the legitimate bank's website and steal the user's credentials.

Spear Phishing

A more targeted attack, where a scammer sends a personalized message pretending to be a colleague or friend, urging a target to click on a link or download an attachment that ends up containing malware.

Smishing

A scam text message claiming a package delivery is delayed, asking a consumer to click on a link to resolve the issue. The link may lead to a fake website or download malware onto a device.

Quishing

Scammers use fake QR codes that lead to malicious websites or steal sensitive data. The fake QR codes could be placed on gas station pumps, parking meters or even restaurant menus and catch consumers off guard.