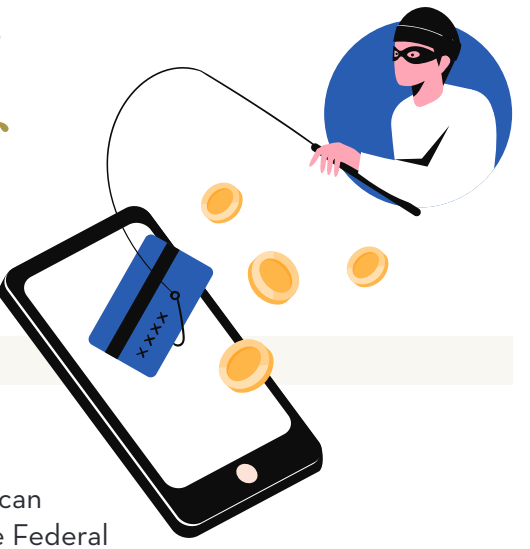
Spring is Phishing Season: How to Protect Yourself from Scammers



BY AIS ELECTRONIC SERVICES COMMITTEE

Spring is awakening across the country and with it a new crop of scammers—some sophisticated and some not so much—popping up. With the preponderance of publicly available information available to scammers coupled with ever more advanced artificial intelligence (AI) features, it is more and more difficult to avoid phishing* attempts. There are, however, steps that you can take to protect yourself.

First, approach all correspondence whether by email or text message with caution. Look for odd spellings, grammatical errors, and logos that are not quite right. Second, is the request, whether for information or financial transactions, rational? If it seems reasonable, and this is a company you do normal business with, contact the company/agency directly either by calling or using their website rather than clicking on any links in the message. Check that the email address or phone number of the sender corresponds to known contacts. On a computer, hovering your mouse over the email address will reveal the actual email address rather than one that might be displayed, does it match your known contact information? On a phone you may need to hit reply to reveal the address, do NOT hit send when using this method to reveal an address. Be aware that phone numbers can be mimicked, always call your contact directly rather than responding to a text message.

Beware of requests that purportedly come from known contacts asking you to buy gift cards that you will then be reimbursed for. Never use a person-to-person (P2P) app such as Venmo or Zelle with someone you do not know well and wouldn't normally have financial dealings with. Phishing attempts using P2P apps are increasing and can result in the instantaneous transfer of funds out of your bank account with no ability to recover those funds.

If you have received phishing emails or text messages you can report it to the Federal Trade Commission's Anti-Phishing Working Group, the information you give helps fight scammers. If you received a phishing email forward it to reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726). To report a phishing attempt to the FTC contact ReportFraud.ftc.gov.

Lastly, if you're suspicious about an email, please do not click on any of the links in the body of the message. A single click may authorize third party access to your computer to malicious individuals who want to have illegal access to your computer.

The American Iris Society, its officers, and its committee chairs will never ask members to buy gift cards or front money through person-to-person (P2P) apps such as Venmo or Zelle for AIS business. If you receive such a request, it is a scam, do not respond to the request. Look up the person's email or phone number on the AIS website at: **irises.org/about-ais/leadership** and send them a separate note that you have been phished. Delete the correspondence from your device after reporting to the FTC.

*A technique for attempting to acquire sensitive data, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or real person.

Information for this article was provided by:
The Federal Trade Commission:
https://bit.ly/IrisesScams1
American Association of Retired Persons (AARP):
https://bit.ly/IrisesScams2