

Phishing - Don't Take the Bait!

FS-2016-08

» As a member of the State of South Carolina workforce, you have access to information that is valuable, and you could be a target of "phishing." Phishing is an attempt to obtain sensitive information, such as usernames, passwords, and credit card details. Phishers may try to pass themselves off as a trustworthy source or imply dire consequences if you do not reply. Below are a few tips to help you avoid taking the bait:

Check links and verify sources of a message.

If an email or text message appears to come from someone you know, but still seems suspicious, forward it to the sender using an address you know to be correct for them, and ask if the message came from them. Most email or text messages can wait a few minutes; set the email aside until you receive the confirmation.

If a message contains a [hyperlink in blue text](#), hover your mouse over the link and the actual web site address should appear. Check before you click!

Question and verify the source when someone asks for information.

Whether by text, email, or phone call, when someone asks for information, make sure you understand who they are before you provide personal details, passwords, or other information. If a request seems unnecessary, ask what the purpose for collecting that information may be. Keep in mind that Caller ID can be forged.

Wear your identification badge when you are at work, and take it off when you leave the office.

ID badges allow us to quickly tell if someone in the workplace should be there, and your ID badge should be worn in the office. When you wear your ID badge outside the office, others can use it to learn information about you to contact you for phishing purposes.

Avoid using personal devices for business, unless authorized by your Agency.

You may receive more unsolicited or unexpected contacts on personal devices than work devices, which can make phishing tougher to spot. Personal devices could be exposed to harmful programs, since you use them to access a variety of sites and applications.

Do not use your personal contact information for business purposes.

Your employer often needs to share your workplace contact information, but that information is less likely to be connected to your personal information or credit reports. By keeping workplace communications through workplace channels, you can ensure a higher confidence in the identities of your contacts and communications.

Ensure you understand your agency's policies, and know whom to contact for more information or assistance.

Each agency will have its own policies and procedures beyond these general best practices. Make sure you know how to act in your specific situation, including under what circumstances to use your agency's help desk.

If you do receive a phishing email, report it.

Let your security, privacy, or IT contacts know if you receive a phishing email or phone call, so those groups can warn others of the tactic. If you are unaware of these contacts, ask your supervisor.



PRIVACY POWER-UP!

What Are

Privacy Power-Ups?

- Tips to **ENERGIZE** privacy program implementation
- Pointers on information privacy safeguards, training techniques, and compliance activities
- Synopses of privacy hot topics, research, and technologies
- Tools for Agency privacy liaisons to increase privacy awareness and establish information privacy protections