

Phishing/Scam Email Notice

phish·ing

/ˈfɪʃɪŋ/

noun

noun: **phishing**

the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

"respondents named ransomware and phishing as leading security concerns"

How to spot a phishing attempt:

Detecting a phishing attempt is often a matter of feeling that something is “**off**” and not quite what it seems, because most phishing attempts are emotional button-pushers. They might appeal to fear (do X or Y will happen), greed (you’re a lucky winner of \$\$\$), curiosity (a file called Salaries.xlsx has been shared with you), perhaps to one’s sense of self and duty (a superior has an immediate need for your assistance), or contain urgent requests (there is a mention of a critical deadline with no time to consider consequences of action).

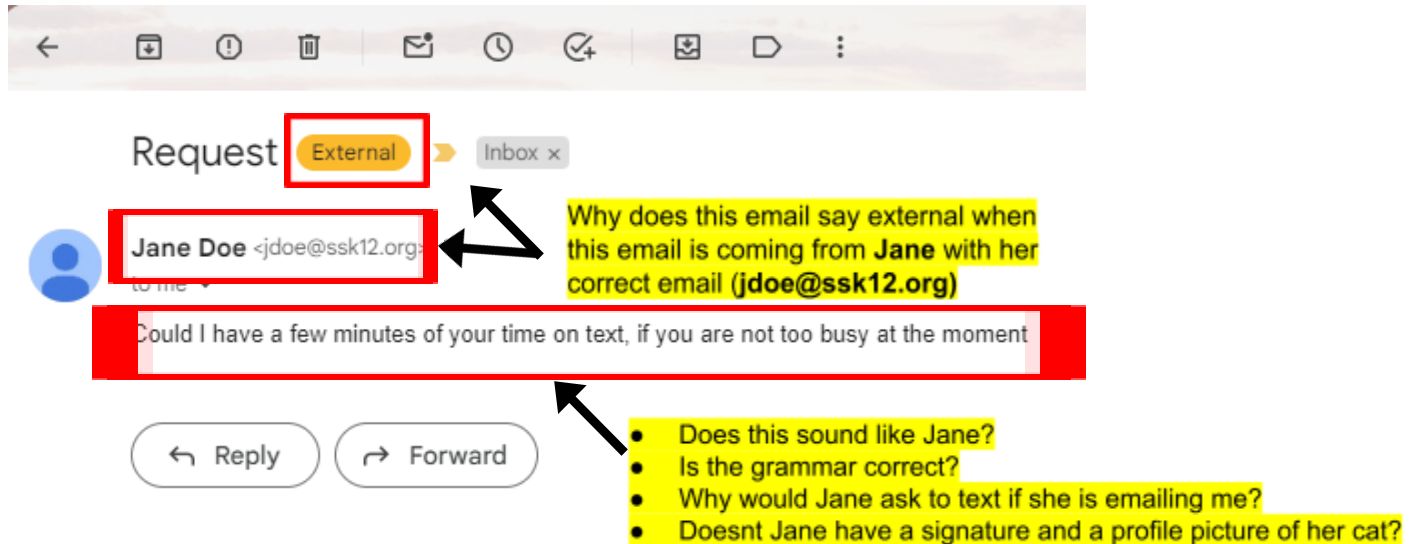
When reading email, here are some traits of a phony and possibly dangerous message that you should be aware of and report immediately, **NEVER** interact with an email you feel is “off” or “wrong”

- The TO field is blank or for another person.
- The email name and address of the SENDER don't match (name is familiar but address is not). These are often called "impersonator" or "spoofing" emails.
- The sender says they are from SSSD but doesn't use their @ssk12.org address.
- It contains an urgent request for an action or information.
- It includes grammatical errors or typos (this is becoming increasingly difficult to spot with the usage of AI tools available).
- It has an offer that seems too good to be true (like a job offer for \$400/week for little work and no experience)
- The message is threatening (Do X right now or lose Y!!!).
- It has a link (or submit button), probably to an unsecured address (NOT https).
- When you hover over the link, it directs you to an address (usually suspicious) other than what is displayed.

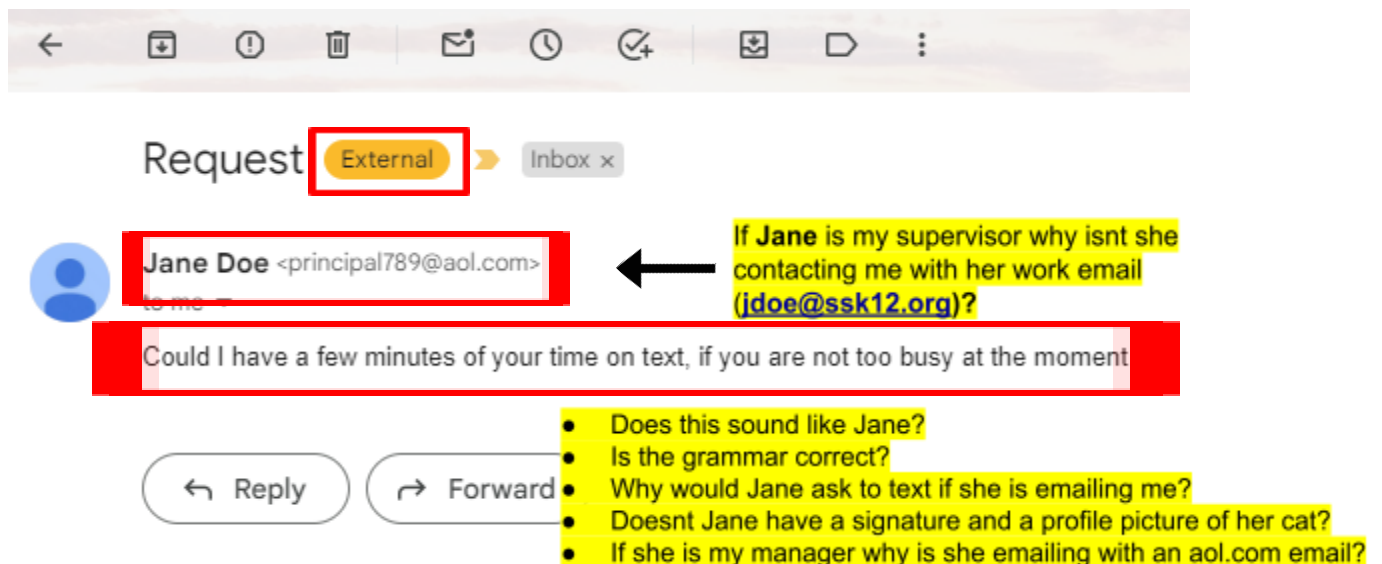
Phishing/Scam Email Notice

Anatomy of a Phishing email

Example 1: Sender address spoofing It looks like jdoe@ssk12.org but it's actually spoofed and coming from criminal@scammersRus.com



Example 2: The email name and address of the SENDER don't match (name is familiar but address is not). These are often called "impersonator" or "spoofing" emails.



If you have any questions or concerns about the authenticity of the email **DO NOT INTERACT** with it. **VERIFY** the sender actually sent the email either in person or by calling a verified number never call or text a number provided in a suspicious email. **REPORT** the email to the IT department and Google.. **DELETE** the email to prevent accidental future interactions.

Phishing/Scam Email Notice

What to do when you spot a phishing attempt:



DON'T INTERACT ■ VERIFY ■ REPORT ■ DELETE

DO NOT INTERACT: If you have any doubts or concerns about the authenticity of the email do not interact with any links, respond to the email, type information into a form or response field, or forward the email to anyone other than IT personnel. This will prevent additional accidental victims.

VERIFY: if you have any doubt about the origin of the email ask the sender in person, call their district 4 digit desk phone extension, call the sender's phone number that is in the Student Information System (SIS) or Payroll/Employee HR system. **DO NOT** call a phone number in the signature or letter head of any messages you believe to be suspicious.

REPORT: If you identify a message to be Phishing, Dangerous in any way or Threatening, inform the IT department ***immediately***. Be sure to mark emails appropriately with Google such as Spam and Reporting Phishing. [Additional information can be found here](#).

DELETE: Delete the email, this prevents you from accidentally interacting with the email in the future.

Phishing/Scam Email Notice

Compromised

If you think you might be the victim of a phishing attempt (or other suspicious email) or are concerned that your account may have been compromised or you may have provided account credentials for any system you should **immediately** contact the IT department for next steps.

What to do if you become a victim of a scam or identity theft

Unfortunately, there is no way for us to track down the scammer. These criminals use fake addresses and relay points around the globe, and usually shut down the servers and addresses in less than 24 hours, migrating to a new one. Major investigations by the FBI on issues like this take years, and often have no results. There are some things you can do. You can start by following the same steps in the previous section. In addition to those, you should:

- Review the Federal Trade Commission site ([ftc.gov](https://www.ftc.gov)) for tips, to file a complaint, and/or log an identity theft concern.
 - > Read [What To Do If You Were Scammed](#) for advice if you paid a scammer, gave one your personal information, or if a scammer has access to your computer or phone.
 - > Go to [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov) to report and fight fraud.
 - > Learn more about [identity theft](#), also on the FTC's site. If you think someone is using your personal information to open accounts, file taxes, or make purchases, visit [IdentityTheft.gov](https://www.identitytheft.gov) to report and recover from identity theft.
- Contact the Attorney General Office from the state you reside and log a complaint.
- Contact the three credit bureaus and place a fraud alert on your SSN (Experian, TransUnion, and Equifax); ask for free credit reports to set as a baseline.
- Note: According to the Social Security Administration, if you have become a victim of identity theft and "you have done all you can to fix the problems resulting from misuse of your Social Security number and someone still is using it, we may assign you a new number." [See their FAQ for details.](#)

Tips from the Federal Trade Commission (FTC)

- [Avoiding and Reporting Phishing Scams](#)
- [How Scammers Tell You To Pay](#) (video)
- [How to Recognize and Avoid Phishing Scams](#)
- [Phishing: Don't Take the Bait](#)