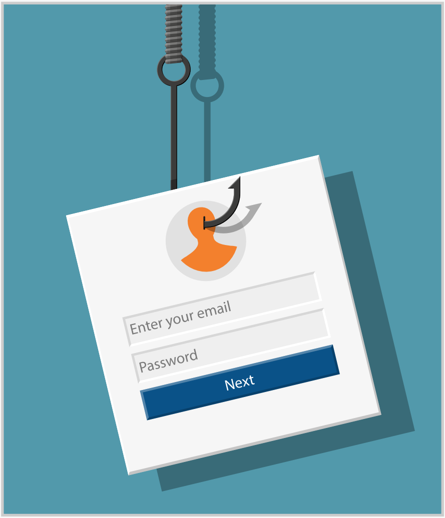
Intrada
TECHNOLOGIES

Watching for Phishing Emails and Scams – 6 Red Flags



Phishing Scams are not new. Phishing was first recognized in the mid 1990s by a hacker named Khan Smith. Smith used the arrow symbols <>< that resemble a fish and commonly used in online chat communications, making it hard for AOL to filter the communications.

In the IT industry, we call these Phishing Scams because they are fishing for information.

So how do you keep from getting caught by Phishing Scams? If you receive an email that you are not expecting or from a sender you do not recognize, it's best not to open it. We suggest you think of it as junk mail and trash it.

'Red Flag' Checks:

LINKS IN THE EMAIL: Links in the body of an email might look valid, but when you click on the link it takes you to a totally different address. If you hover over the "baited" link, most browsers will display the actual link you would be directed to in the bottom left corner.

EMAIL ADDRESS: Spammers use what is called "Spoofing" to present you with an email address that looks convincing, but it's actually hiding the bogus email account.

ABC **GRAMMAR:** Most scams have incomplete sentences, poor grammar, and lack of customer brand and contact information.

ATTACHMENTS: Scammers will attach files that, when opened, will try to install malware and infect the computer. The best protection is not to open any attachments that you didn't expect or were not sent from a valid source.

FREE SITES: Avoid websites that require you to install an application to access free files including fonts, music, videos, games or other applications.

HELP DESK: Contact Intrada's Help Desk to have any emails checked before opening.

HOT RULE

Do not enter your user name and password on any websites that were linked from an email.