GONE PHISHING?
DON’T EAT THE SPAM!

Prelude strives to maintain a highly secure network environment and has proactive tools in place to block the majority of suspicious email, please remember that you are also an important part of that defense. If you do receive unsolicited email, collectively referred to as SPAM, we highly recommend that you do NOT open the email.

What is SPAM?
Email SPAM, also known as junk email or unsolicited bulk email, is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. The messages may contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments.

What is Phishing email?
These emails try to look like they’re from a person within your organization and someone you may know. They may ask for your personal information, such as credit card number, social security number, account number or password. To help you determine if an email is from a person within your organization, Prelude has implemented an “[EXTERNAL]” subject notification in the Subject line of your emails.

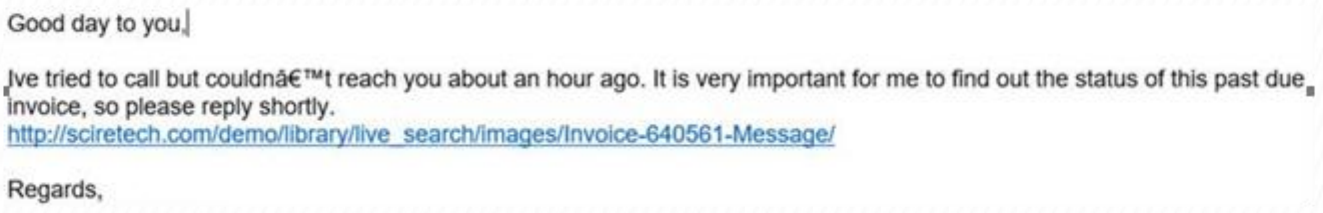
Ways to determine “FAKE” email: (See example below)

Email messages sometimes contain poor spelling and grammar.

They often ask you to reply to the message with confidential information.

They have an urgent tone and threaten account suspension if you don’t pay or update your information right away.

Here’s an example of a Phishing Email:



Good day to you,

Ive tried to call but couldnâ€™t reach you about an hour ago. It is very important for me to find out the status of this past due invoice, so please reply shortly.
http://sciretech.com/demo/library/live_search/images/Invoice-640561-Message/

Regards,

Not all “[EXTERNAL]” email is “FAKE” email, this is only a way to identify that it came from outside your organization. It is important that all users be vigilant and know what to do if receiving email that is not familiar to them or otherwise looks suspicious.

What should I do when receiving SPAM or Phishing email?

If you receive spam or phishing email, you should ignore and delete them, this is the simplest and most effective way to handle SPAM and Phishing email.

If it looks suspicious, delete it.

Never reply to spam or phishing emails or click on any links contained in the email.

INNOVATIVE. SECURE. IT SOLUTIONS.
www.preludeservices.com
800.579.1047