Banner Health

SPOTTING SUSPICIOUS EMAIL: PHISHING & SPAM

RECOGNIZING SUSPICIOUS EMAIL IS EASY IF YOU KNOW WHAT TO LOOK FOR!

65% OF EMAILS SENT ARE SPAM *

TWO TYPES OF SUSPICIOUS EMAIL

—PHISHING —

Phishing occurs when emails solicit you to enter personal information by posing as a trustworthy source

The goal of a phishing attempt is to trick you into providing sensitive information, such as log in credentials, so that the cyber intruder can access your data and potentially the corporate system

VERSUS

— SPAM —

Spam is unsolicited electronic messages sent to a large number of recipients or posted in a large number of places. Most often these appear as email, but can also appear as text messages, or Internet postings

Spam is annoying, and it can be dangerous! Spam can contain malware, viruses, and dangerous links

Phishing scams are a dangerous threat and should be immediately reported by emailing:

reportphishing@apwg.org

DO NOT
- CLICK LINKS
- OPEN SPAM
- CLICK THE UNSUBSCRIBE BUTTON

If you think a message is spam, send it to your junk mail and block the sender

— SIGNS OF A SUSPICIOUS EMAIL —

1 URGENCY

2 SPELLING & GRAMMAR ERRORS

3 REQUEST FOR LOG IN CREDENTIALS

4 UNUSUAL SENDER / REPLY TO ADDRESS

To: employee@workplace.com

Subject: URGENT!!!!! Respond Now!!!

Greetings and Salutations,

Your pssword is about to expire. You will be locked out if you do not respond today!!!!

Please send your username and password to IT@yourwork.yw.net.

Thank You,

Information Security

*HIPAA Journal, Feb 3, 2017

For more information, please visit https://education.apwg.org