12 SOCIAL ENGINEERING RED FLAGS

Cyber criminals send emails to manipulate people into giving them information, money, and/or access.

What are the warning signs?

STRANGE ATTACHMENT

The email has an attachment that you were not expecting or that makes no sense.

DANGEROUS FILE TYPE

The email includes a potentially dangerous file attachment. The only file type that is always safe is .txt

UNUSUAL DATE

The email looks normal but it was sent at unusual time like 4 AM.

UNKNOWN SENDER

The sender is someone you don't normally communicate with.

RIGHT SENDER, WRONG MESSAGE

The email is from someone you know but is very unusual or out of character.

SUSPICIOUS DOMAIN

The sender is from a strange or subtlely misspelled domain like mircosoft-support.com

RANDOM AUDIENCE

You are cc'd on an email sent to people you don't know or an unusual mix of people you do know.

SUBJECT MISMATCH

The email subject line doesn't match the content or is a reply to something that you never sent.

STRANGE CONTENT

The body of the email is odd. Watch out for bad grammar and spelling errors.

ACT NOW!

The sender is asking you to click on a link or open an attachment to avoid a negative consequence or gain something of value.

DIFFERENT LINK ON HOVER

When you hover your mouse over a hyperlink in the email body, the link-to address is for a different website.

MISSPELLED HYPERLINK

The email contains a misspelling for a known website like www.bankofanerica.com.

TCG Network Services

Implementing Technology that Empowers People