TRINITY WORLDWIDE TECHNOLOGIES, LLC

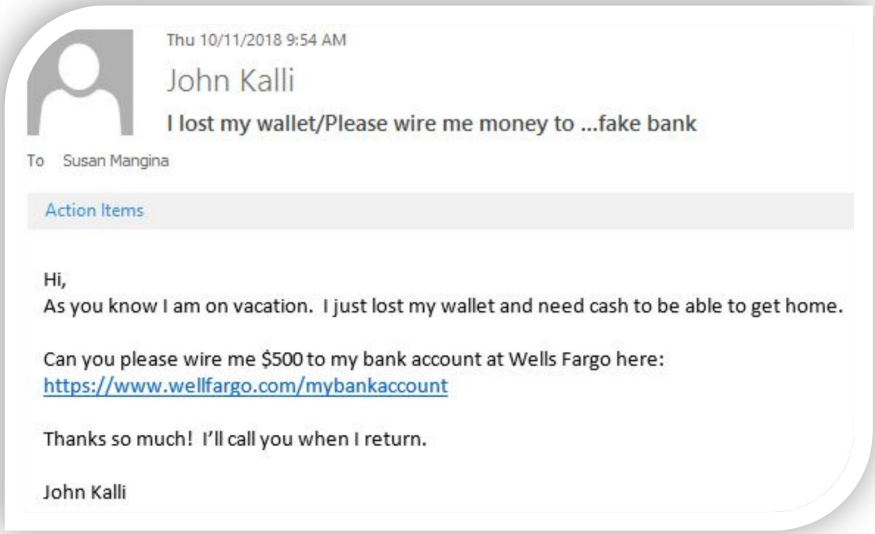
SOCIAL ENGINEERING RED FLAGS

The Human Component - The human layer of information security is all about **teaching people** to spot scams and be cautious with important information.

Be aware of the **Red Flags**! (*Here are a few*)

FROM:

- **The email can appear to be from someone you communicate with, but the request is out of character**
- **Or someone that you do not typically communicate within your organization**
- **An unexpected email with attachments or an embedded hyperlink from someone with whom you have not recently communicated.**



To:

- **I don't know the other recipients or I was cc'd**

Subject:

- **An odd request or info that you haven't requested**

Content:

- **Asking you for personal information or telling you that you won something**
- **False urgency! Out of the ordinary/change your password/someone you know is in trouble and in need of your assistance**
- **Bad grammar/spelling errors**

Hyperlinks:

- **Incorrect/misspelling in hyperlink (example here – *misspelled Wellsfargo.com*)**
- **Tip: Hover over hyperlink to see that it leads you to a different site**

Attachments:

- **Beware of opening any attachments that you are not expecting.**

No one wants to become a victim of a social engineering attack, so it's important to recognize an attack in progress and respond to it appropriately. Better to be safe than sorry!

TRINITY WORLDWIDE

Trinity Worldwide Technologies, LLC
Tel: 732-780-8615
sales@trinityww.com

Microsoft Partner