Why can email attachments be dangerous?

Some of the characteristics that make email attachments convenient and popular are also the ones that make them a common tool for attackers:

- **Email is easily circulated** - Forwarding email is so simple that viruses can quickly infect many machines. Most viruses don't even require users to forward the email—they scan a users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.
- **Email programs try to address all users' needs** - Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.
- **Email programs offer many "user-friendly" features** - Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any viruses within the attachments.

What steps can you take to protect yourself and others in your address book?

- **Be wary of unsolicited attachments, even from people you know** - Just because an email message looks like it came from your mom, grandma, or boss doesn't mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes email messages that appear to be from your ISP or software vendor and claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.
- **Keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it. (**At York this happens automatically**)
- **Trust your instincts** - If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the anti-virus software might not have the signature. (**Contact IT and have them verify the source or block it if necessary**). However, especially in the case of forwards, even messages sent by a legitimate sender might contain a virus. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.
- **Save and scan any attachments before opening them** - If you have to open an attachment before you can verify the source, take the following steps:
  1. Contact York IT Service Desk ext. 5311
  2. Do not save the file.
  3. Let IT determine the threat level and treatment moving forward.
- **Turn off the option to automatically download attachments** - To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.

Produced by US-CERT – http://www.us-cert.gov Authors Mindi McDowell and Allen Householder

The below chart shows how attackers and cyber criminals use social engineering to get you to click on links and open attachments in email. Information provided by KnowBe4.com

Social Engineering Red Flags

FROM:

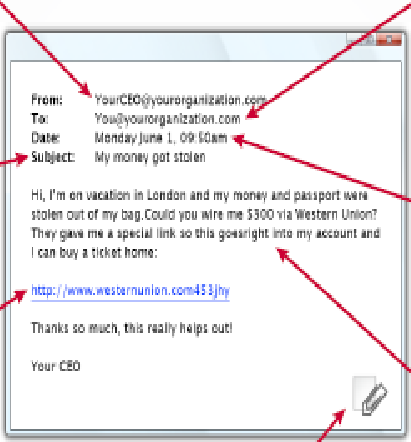
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address **from a suspicious domain**? (like micorsoft-support.com)
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.

TO:

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance a seemingly random group of people at your organization whose last names start with the same letter, or a whole list of unrelated addresses.

SUBJECT:

- Did I get an email with a subject line that is **irrelevant** or **does not match** the content?
- Is the email message a reply to something I **never sent or request**?



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday June 1, 09:50am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag.Could you wire me $300 via Western Union? They gave me a special link so this goesright into my account and I can buy a ticket home:

http://www.westernunion.com453jhy

Thanks so much, this really helps out!

Your CEO

DATE:

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

HYPERLINKS:

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different web site**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters – "r & n")

CONTENT:

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence**, or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

ATTACHMENTS:

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me these types of attachment(s).)
- I see an attachment with a **possibly dangerous file type**. The only file type that is **always safe to click on is a .TXT** file.)

KnowBe4.com
Human error. Conquered.