CITY OF BRYAN

The Good Life, Texas Style.™

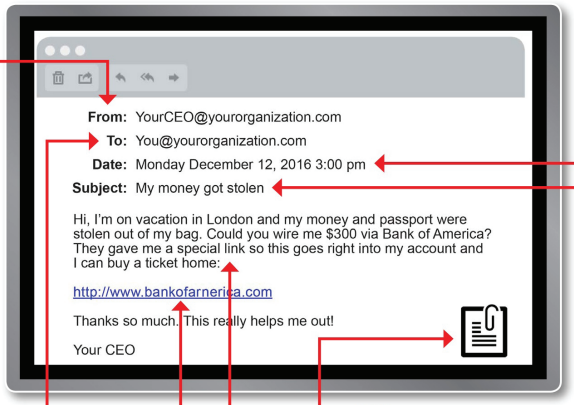
ONLINE SAFETY IN THE WORKPLACE

Here are the Top 5 things YOU can do to help the City of Bryan stay cyber safe:

CHAMPION
National Cybersecurity Awareness Month

1 **What does a cybersecurity expert really do? *Know YOUR red flags!***

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 haven'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, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (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" and "n."

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.?

SUBJECT

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

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 this type of attachment.)
- 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.

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?

KnowBe4
Human error. Conquered.

ONLINE SAFETY
IN THE WORKPLACE

CHAMPION
National Cybersecurity Awareness Month

2 Manage YOUR password like a pro.

Recommendations

- Do not use YOUR password for multiple accounts. Recently there was a breach at Facebook where millions of passwords were disclosed. What if YOU were one of them and YOU used same login for Facebook and YOUR bank's website? Usernames and passwords from this breach are for sale on the dark web for only $2 to $3.
- Make YOUR password long. Each character added to a password can add days to years of time it would take for a computer program to discover YOUR password.
- Do not use a common phrase. Do not use song lyrics, poem versus, YOUR kids' names, birthdates, or Bible verses, anything that more than just YOU knows.
- Do not store passwords in YOUR browser.

Password safes (*NOTE: I am not making an endorsement on any one of these*)

- KeePass - https://keepass.info/
- LastPass - https://www.lastpass.com/business-password-manager
- DashLane - https://www.dashlane.com/
- PasswordSafe - https://pwsafe.org/
- 10 Best Password Managers of 2018

3 If YOU care, do not share.

Have YOU ever played the game Twenty Questions? Just like the game, hackers can gather information about YOU and they have nothing but time. They troll social media and learn… who YOUR friends are, if YOU have Pets, YOUR favorite sports team, YOUR favorite band. With this information, they can impersonate someone YOU know or use that information to impersonate YOU to attack someone else.

- Don't share too much on social media. Too much information will make YOU an easier target for a focused attack.
- Verify YOUR friends.
- Be suspicious of people reaching out to YOU that YOU do not know.
- Hackers can use profiles and posts from several social media apps to create to sophisticated attacks against YOU, YOUR family, YOUR friends and the City of Bryan.

4 Know YOU are a target.

- We will protect YOU to an extent but there are so few of us and so many of them. YOU must step up to protect YOURSELF, YOUR family, YOUR co-workers, and the City of Bryan.
- YOUR actions make a difference. So, if YOU see something that looks off or does not feel right let someone know.

5 Accidental Data loss/exposure.

- Watch auto complete with emails. Have YOU ever accidentally sent an email to the wrong person or to a whole group of people? Email contains information for a target audience. However, not paying attention to who YOU are sending the email to can cause privacy violation and/or embarrassment for YOU and the intended audience.
- Use a pin/passcode on YOUR mobile devices in case YOUR devices are lost/stolen. It will make it extremely difficult for the individual that has YOUR device to access data.
- Always look for YOUR device when leaving. Ever leave YOUR phone somewhere? When leaving a car, restaurant or any place, check YOUR location to see what YOU left behind.
- Place a point of contact sticker on YOUR device. If YOU do lose YOUR device, a good citizen can use this information to return it to you. Place a sticker on YOUR phone with contact details or I.C.E. (In Case of Emergency) information. If YOU are injured and no one around knows YOU, the rescue workers will be able to contact the appropriate people quickly and easily.

UPCOMING TRAININGS: Facebook Friends, Workplace Enemies • John Romero's Trainings