Protect Yourself Online –

Your Online Safety and Security Is Important To Us

Keeping your information secure is a team effort. City National Bank (CNB) can provide you and your business with additional tools and information to help you keep your information protected. If your computer is compromised, hackers may gain access to your personal information, such as your bank accounts, personal emails, or social security number.

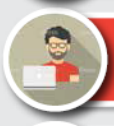
We recommend that you use Trusteer Rapport, provided for FREE, when using Online Banking or ePartner. Trusteer Rapport will help block malicious attempts to access your account or personal data, all of which is targeted at stealing your money. In addition, Trusteer Rapport will not only help protect your online banking activity with CNB, but it will also protect other confidential transactions from other malicious malware. For enhanced protection, combine Trusteer Rapport with your current anti-virus or security software.

Identity theft is one of the fastest growing ways criminals can fraudulently obtain money without fear of being caught.

Fraudsters do not discriminate and will attack any age, gender, or race.

10

For every ten fraudulent e-mails, fraudsters have a 90% chance of gaining access to at least one account.



Attackers have more than 7,900 ways to access your information through security vulnerabilities in the software you may use on a daily basis.

In 2015, the Internal Revenue Service said that more than 300,000 taxpayer accounts were potentially affected by fraudulent activity.

DOWNLOAD TRUSTEER

We recommend that you use Trusteer Rapport. This will not only protect your online banking activity with CNB, but it will also protect you from malicious attacks such as man-in-the-browser, DNS hijacking, and key loggers.

HOW TO DOWNLOAD TRUSTEER?

Trusteer is easy to download and easy to use. Just visit citynational.com and visit our Online Services page. Once you select the Trusteer link, you will find more information regarding how to download Trusteer.

You may also contact us at 305-349-5465, Monday through Friday, 8:30 AM – 5:00 PM.

E-mail is one of the easiest ways fraudsters can gain access to your personal information. Either through a link, attachment or fraudulent request, e-mails are full of potential risks. Below are some E-MAIL RED FLAGS you should become familiar with. Hackers are creative with their fraud attempts, so be careful when conducting any business online.

FROM:

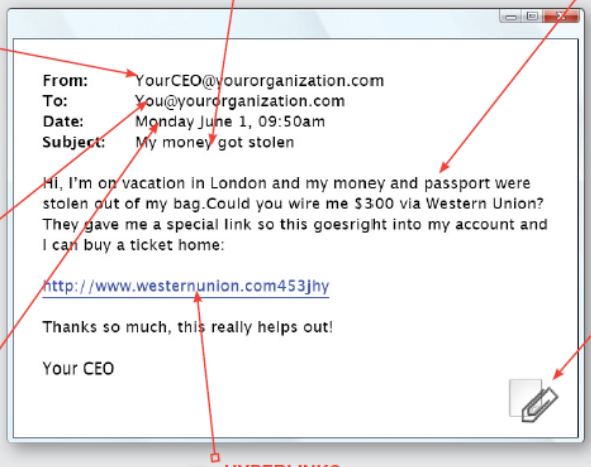
- I don't recognize the sender's email address as someone **I ordinarily communicate with.**
- This email is from **someone outside my organization and it's not related to my job responsibilities.**
- This email was sent from **someone inside the organization** or from a client, vendor, or partner and is **very unusual or out of character.**
- Is the sender's email address **from a suspicious domain?** (like micorsoft-support.om)
- **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 communication** 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 requested?**



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 **suspicious?**
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- The fraudster can spoof an email address of someone you may know so if it looks suspicious or out of character, it probably is.
- 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.)

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 the 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.bankofamerica.com - the "m" is really two characters – "r & n"