Security Awareness
Part I
Tips for protecting your accounts and identity from cybercrime

Carthage College
2017

CARTHAGE COLLEGE

Step 1:

Don’t Get Hacked!!

Learn to recognize phishing attempts and other dangerous content.

Here’s how...

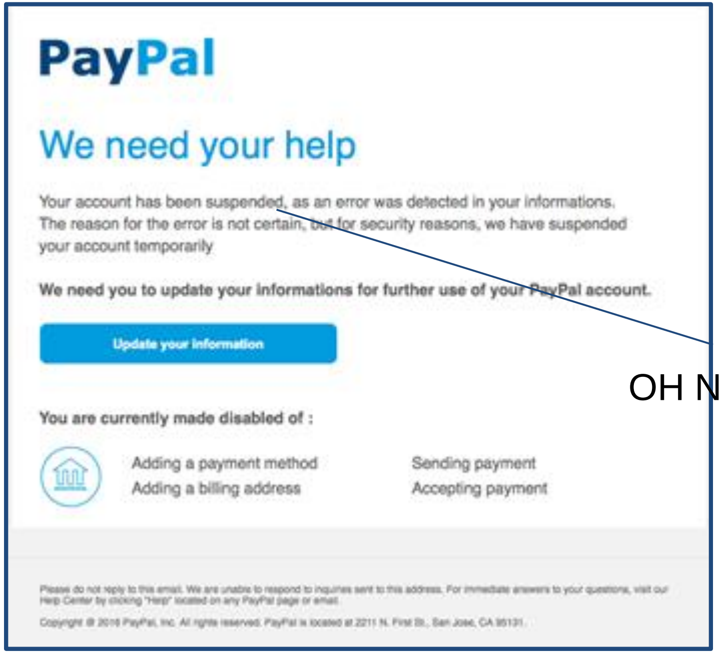
Lures belong in your tackle box,
NOT your inbox.

DON'T LET A **PHISHING SCAM** REEL YOU IN

In a phishing scam, a criminal sends you an email message that appears to come from a legitimate source, like your bank or some other reputable company. The message, which may look authentic, instructs you to follow an enclosed web link—usually to "confirm your account" or "verify your information immediately." But the link actually sends you on to a counterfeit website that looks like the real one.

Delete suspicious messages immediately, and NEVER respond to email requests for personal information.

Have You Seen These???



PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

You are currently made disabled of :

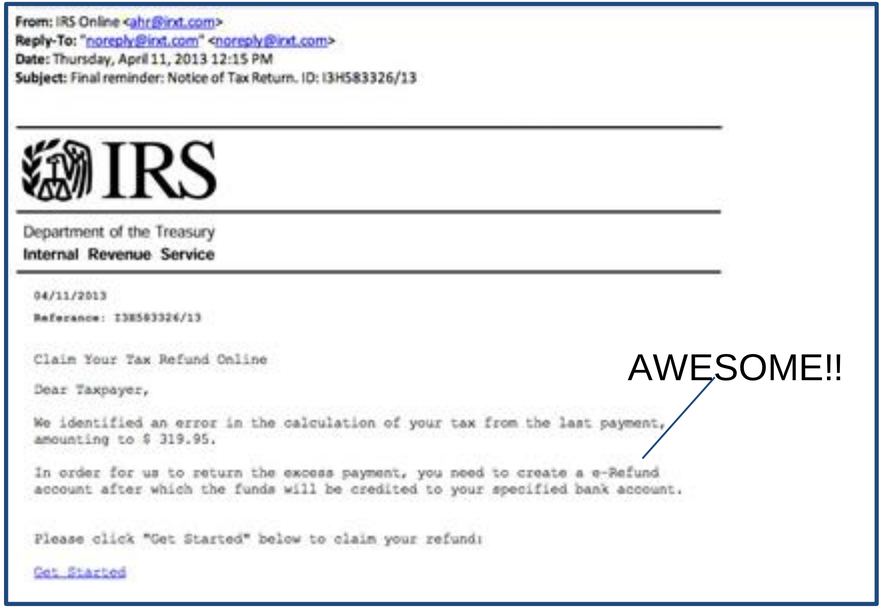
Adding a payment method
Adding a billing address

Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright © 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

OH NO!!!



From: IRS Online <ahr@irxt.com>
Reply-To: "noreply@irxt.com" <noreply@irxt.com>
Date: Thursday, April 11, 2013 12:15 PM
Subject: Final reminder: Notice of Tax Return. ID: I3H583326/13

IRS

Department of the Treasury
Internal Revenue Service

04/11/2013

Referance: I3H583326/13

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $ 319.95.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

AWESOME!!

What Phishing Attacks Can Do

- Obtain your password or other data for other malicious use
- Introduce malware that can steal, alter, or destroy your data such as:
  - –Viruses
  - –Adware
  - –Spyware
  - –Ransomware

What if hackers get a hold of your password?

Theft

Infiltration

Stolen Identity

Damage to Reputation

Data Destruction

- They could try your password on other sites like Amazon, your bank, PayPal, and others.
- They can USE your email to change your banking and online passwords for other sites and then buy things, request credit cards, transfer your money, etc.
- They could send a hate email to a prominent politician in your name, and the FBI will come visit you
- They can get access to any Carthage systems that you normally have access to.
- They can send the next round of phishing emails from your account.

Identify Phishing Attacks

How they get you …

– **They pose as a reputable entity to try to get your information or infect you.**

– **They are convincing!!** Don’t be duped by aesthetics. Phishing emails often contain convincing logos, links to actual company websites, legitimate phone numbers, emotional appeals, and e-mail signatures of actual people you know.

– **Be especially aware of messages with spelling and grammatical errors**, as reputable organizations do not send emails with spelling and grammatical errors.

Don’t take the bait!!

Spear Phishing

- Targeted phishing messages.
- Often are researched using content from LinkedIn, Facebook and other public information to tailor the spear phish method.
- Often aimed at executives and administrators with privileged access.

Vishing

- “Voice Phishing” uses the phone to contact you.
- Often spoof a reputable source such as Microsoft or the IRS.
- Offer to help you solve a problem such as computer errors or back taxes.

Main Methods of Attack

Beware of phishing scams.
Don't take the bait! Be suspicious of anyone that asks for your personal information.

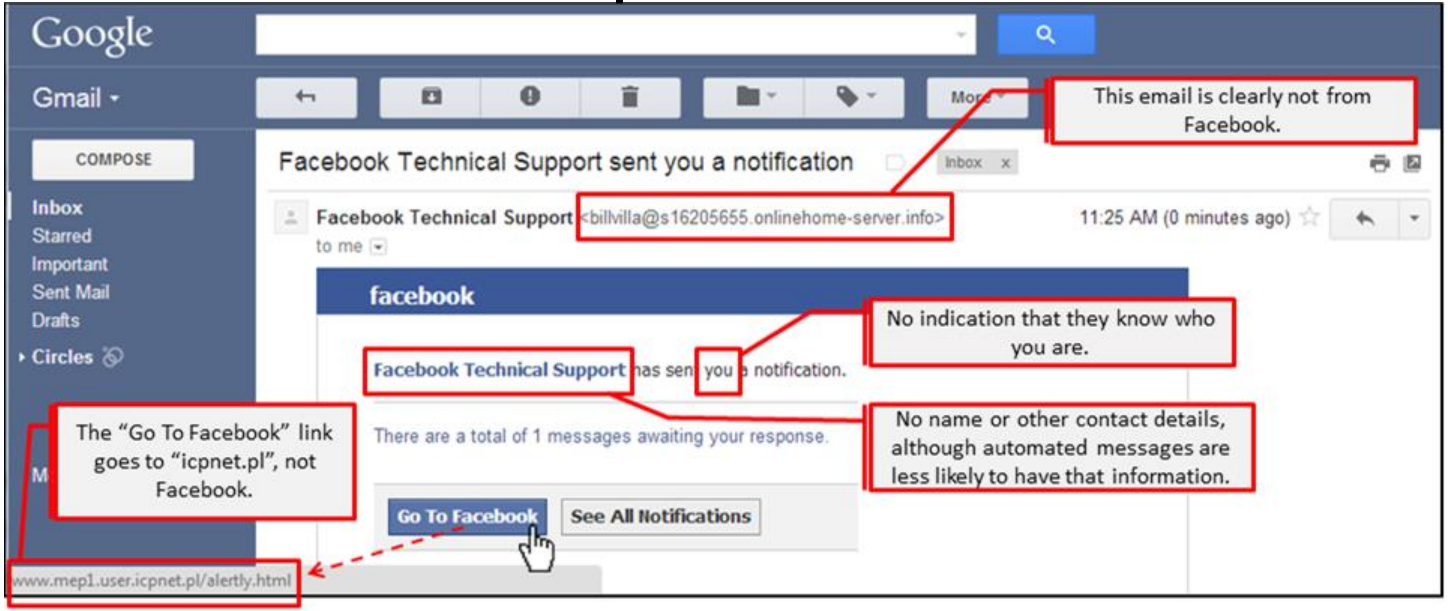
- Malicious attachments, which contain the initial exploit
- Web redirection: requesting that you fill out a form

Protect yourself from Phishing

- **Be Suspicious**. If the message is urging you to take action — especially sending sensitive information, clicking a link, or downloading an attachment, or sharing information on the phone
- **Avoid carelessly opening links and attachments.** Confirm URLs. Don’t open attachments unless you’re expecting a file from someone.
- **Don’t give them material to work with.** Maintain tight social media security and privacy settings.
- **Verify the sender.** Check the sender’s e-mail address to make sure it’s legitimate. If it’s someone you know, ask if they really sent it.
- Go directly to the site and see if the offer or notice is there

CARTHAGE COLLEGE

A Suspicious Email



Facebook Technical Support sent you a notification

Facebook Technical Support <billvilla@s16205655.onlinehome-server.info>
to me

11:25 AM (0 minutes ago)

facebook

Facebook Technical Support has sent you a notification.

There are a total of 1 messages awaiting your response.

www.mep1.user.icpnet.pl/alertly.html

This email is clearly not from Facebook.

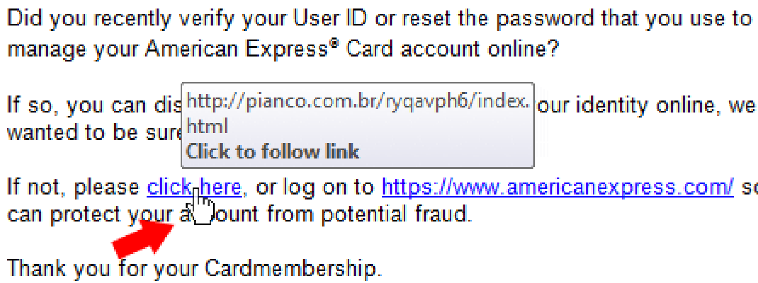
No indication that they know who you are.

No name or other contact details, although automated messages are less likely to have that information.

The "Go To Facebook" link goes to "icpnet.pl", not Facebook.

- **They pose as a reputable entity to try to get your information or infect you.**
- They often use malicious attachments, which contain the initial exploit or web redirection (not just .exe)
- They might request that you fill out a form to capture additional data

Things to Check



Did you recently verify your User ID or reset the password that you use to manage your American Express® Card account online?

If so, you can dis our identity online, we wanted to be sure

http://pianco.com.br/ryqavph6/index.html
Click to follow link

If not, please click here, or log on to https://www.americanexpress.com/ so can protect your a ount from potential fraud.

Thank you for your Cardmembership.

- Web redirection:
  - Identifying the components of the address
  - Hover over the link to see the URL
  - Use a site like Norton Safe Web to determine site safety (more later)
- Malicious Attachments
- Go directly to the site and see if the offer or notice is there
- Contact the ‘sender’ to verify (email directly rather than replying)

Ways to check on a URL

- Use Safeweb.Norton.com to paste in a url and find out if it has security risks
- Search the web site name with ‘scam’ to see if scams have been reported
- Note shortened URLS (ie Bitly – shortened URLs) need 2 steps:
  - Use Unshorten.it to get the full site
  - Then check Safeweb.Norton.Com

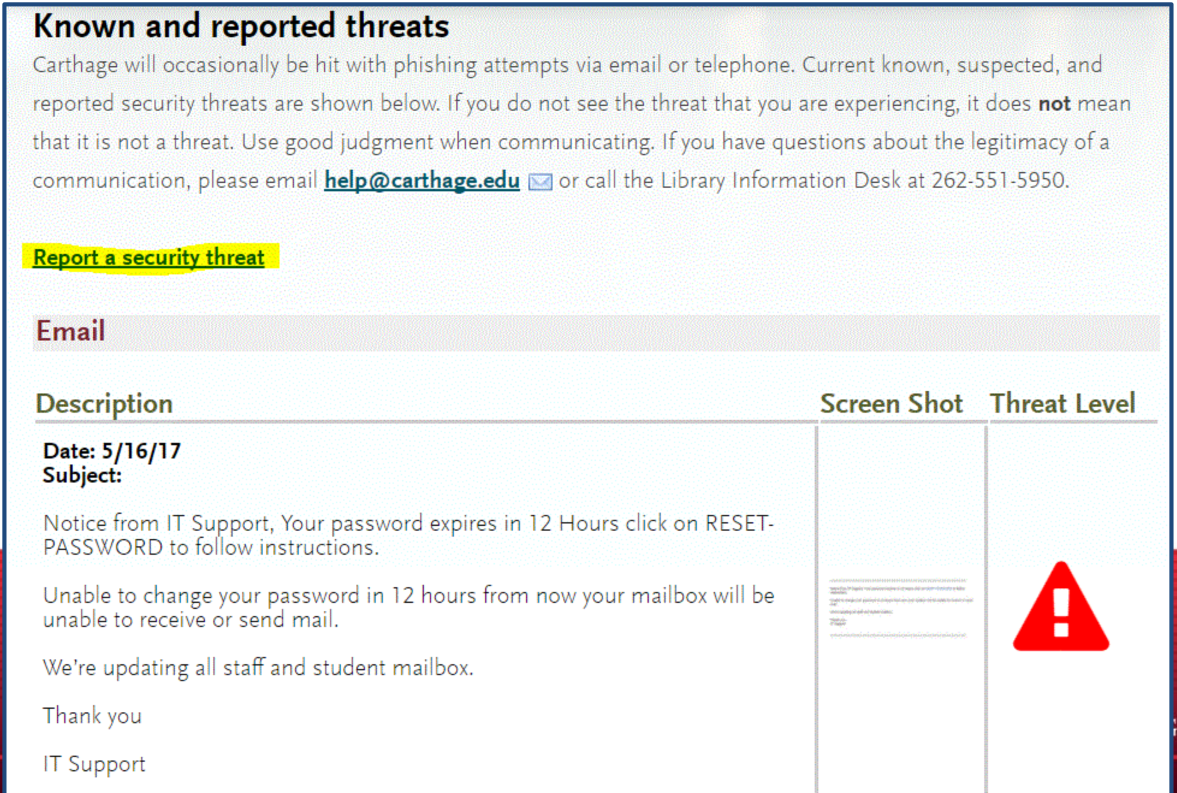
Reporting a Phishing Email

Go to https://www.carthage.edu/library/internet-security-threats/

See if your threat is already reported

Click the "Report a security threat" link

Fill out the form



Known and reported threats

Carthage will occasionally be hit with phishing attempts via email or telephone. Current known, suspected, and reported security threats are shown below. If you do not see the threat that you are experiencing, it does **not** mean that it is not a threat. Use good judgment when communicating. If you have questions about the legitimacy of a communication, please email **help@carthage.edu** or call the Library Information Desk at 262-551-5950.

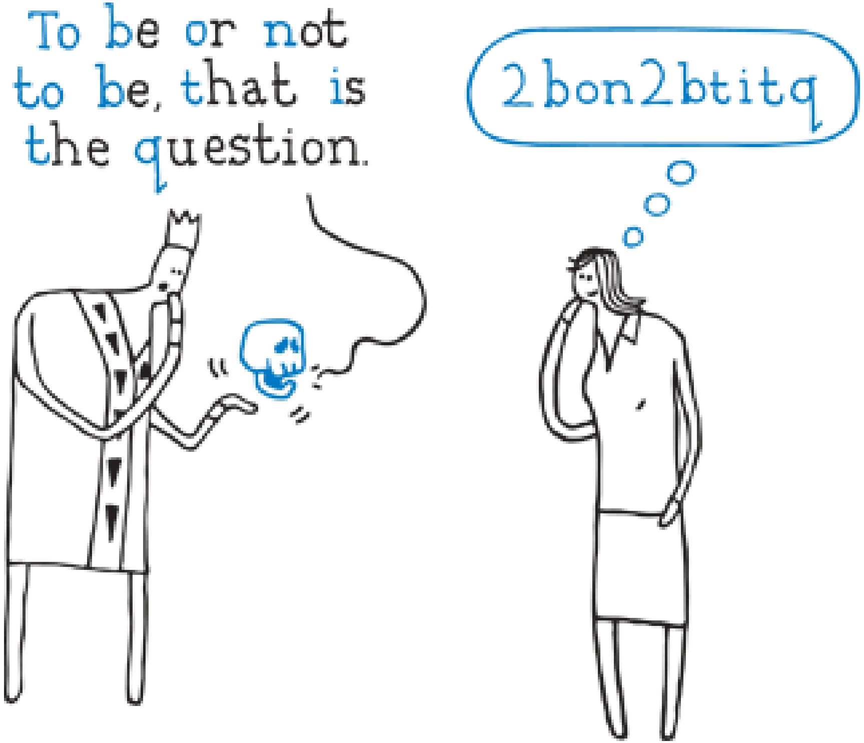
Report a security threat

Email

Description	Screen Shot	Threat Level
Date: 5/16/17 **Subject:** Notice from IT Support, Your password expires in 12 Hours click on RESET-PASSWORD to follow instructions. Unable to change your password in 12 hours from now your mailbox will be unable to receive or send mail. We're updating all staff and student mailbox. Thank you IT Support		⚠

Step 2:

Select a great password and keep it safe!



Create Strong Passwords

1. Use good Passwords/Passphrases: **12 or more characters in length** LONGER PASSWORDS ARE BETTER!!!!!

1. **Don't make sense!** -Don't use information about yourself or your life that would could be looked up. That includes the names of your pets, your hometown, the name of your spouse or significant other, etc.

   -Avoid quotes or names of characters from pop culture
   -There's no reason for your password to make sense. Passwords that make sense are easier to predict, easier to crack

Create Strong Passwords (cont'd)

4. **Make an alphanumeric password with symbols**
   Use numbers, letters (upper & lower cases), and symbols.

4. **A password doesn't need to have only one word**.
   String multiple, unrelated words together with numbers and symbols.

artikokeb52feathers$
String of Artichoke (misspelled),
b52 & feathers

$rmntgtstosn80$
Remind Me Never to
Go To State Fair on
Saturday Night

nOOnioninmysmoothy.
no onion in my
smoothie (misspelled)

Don’t Weaken your Passwords!

- You should never have two accounts with the same password!
  - If one account is compromised, the other will be compromised as well.
  - Hackers count on people using the same password for multiple accounts.
- Treat important accounts (e.g., bank accounts) with extra care.
  - Use separate browsers for work and play.
  - Clear your browser history before logging into an important account.

Manage Your Passwords

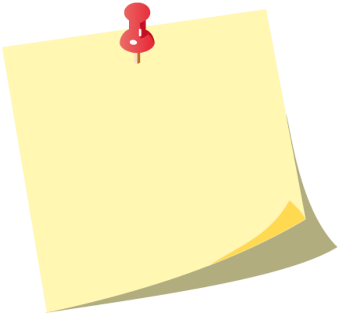
Don’t let browsers store your passwords for you.

Google Chrome, Firefox, et al., don’t require a password to view your stored passwords. If you forget to lock your computer, someone could open your browser and write down all of your unprotected passwords.

Don’t write your passwords down and store them near your computer.

When it comes to password security,

Post-it notes are not your friends.



Carthage's New Password Policy

12 or more

- Because password length is the biggest contributor to password strength, the minimum password length will increase to 12 characters

- We will also expand the time between password resets to 180 days, requiring a less frequent updates

You can go to password.carthage.edu *to reset your password now to comply with the upcoming change*

Step 3:

Beware of Public WiFi

Dangers of Public Wifi

Lack of Encryption

Packet Sniffing

Fake Access Points

Session hijacking

Limit use of public Wi-Fi

- Be skeptical of ALL free public WiFi (specifically *TWCWiFi*, *attwifi*, and *Free Wi-Fi*)
- Check the authenticity -- ask the owner of the hotspot for correct network name and password - its easy for hackers to set up hotspots with similar names
- If utilizing public WiFi, avoid using any sites that transmit personal or sensitive information (i.e., email, online banking, shopping, etc.)
- Utilize a secure VPN connection when on public WiFi

Limit use of public Wi-Fi, cont'd

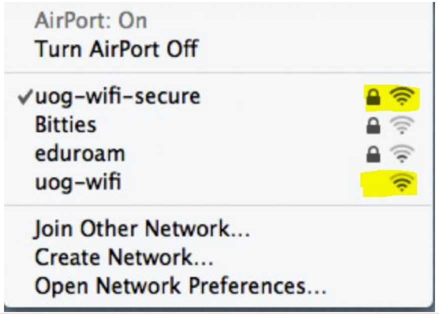
–'Forget' the network on your device once you are done with it

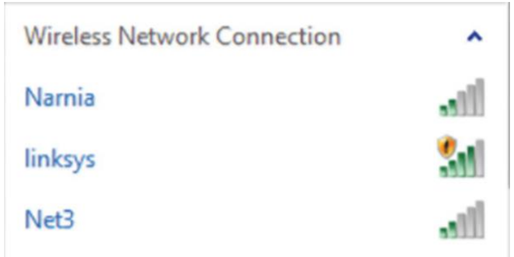
–Turn off WiFi when you are not actively using it

–Choose encrypted networks when using public Wi-Fi (i.e., choose password-protected (secure) networks when possible)

Secure network in OS X

Unsecure network in OS X





Secure network in Windows

Unsecure network in Windows

Carthage-Open vs.Carthage-Secure

- The College maintains two wireless SSIDs; Carthage-Open and Carthage-Secure (anything else is not ours!)
- Carthage-Open offers no encryption
- Carthage-Secure offers full encryption with the latest authentication and encryption standards (EAP, WPA2-CCMP)
- Carthage-Secure should be used by all faculty, staff and students on all devices
- Carthage-Open should only be used as a last resort; otherwise, it should be used by Guests only

Step 4:

Enable Multi-Factor Authentication

Also called “2-step verification”
or “2-Factor Authentication”

Protects your accounts even if your password is compromised

AWESOME Security Feature!!!

Easiest way to protect yourself from remote hackers

Requires you both have ‘something you know’ <password>
AND
‘Something you have’ - a phone, a list of codes, etc

Offered by banks, google, etc
Google’s is called ‘2 Step Verification’

Carthage’s Plans

- Carthage will be implementing this technology for Google and VPN in the near future
- You can turn on Google’s 2-Step Verification Now

Looking for More Information?

Go to **Ask Albert**: https://albert.carthage.edu/

Albert Article #1424

How do I turn on

Google's 2-Step

Verification?

CARTHAGE
COLLEGE

Step 5:

Ensure Device Security

Device Security Overview

Ensure

- Security of the physical device.
- Recovery of the device if it’s lost or stolen.
- Security of the data sitting on the device, e.g., encryption.
- Security of any backups of that data.

General Tips

- Ensure all software is up-to-date. Turn on automatic updates where possible.
- Lock your device whenever you walk away from it
- Physically secure your laptop to reduce theft
- Encrypt your hard drives
    - All Carthage-owned hard drives will be encrypted moving forward

Looking for More Information?

1. Go to **Ask Albert**: https://albert.carthage.edu/
2. **Passwords and Security** section on the left.
3. Article titles & ID numbers below...

Albert Article ID#1472

Android Security

Albert Article ID#1474

iOS Security

Albert Article ID#1471

macOS Security

Albert Article ID#1473

Windows Security

CARTHAGE
COLLEGE

Next Steps

- Set your Carthage password to 12 characters or more
- Turn on Google 2-Step Verification (Ask Albert Article #1424)
- Read the new IT Security and Acceptable Use of Technology Policy - Employees -> Carthage Policies
- Attend IT Security@Carthage

Questions?

Always better to ask!

Email to help@carthage.edu

or ask us now…