PHISHING 101

HOW TO DETECT FRAUDULENT EMAIL

GEORGIA COLLEGE INFORMATION SECURITY OFFICE

Hance Patrick, ISO
Information Technology
Summer 2018

OVERVIEW

- **Phishing** is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers
- Phone fraud has been around since the dawn of telephones; many callers will purport to be from the IRS, your bank or lending institution, or your company
- Email / Phishing: Extremely easy to deliver, inexpensive, nearly no time invested

EMAIL SPOOFING

- Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source
- Can be done easily and can appear to be sent from ANYONE. Examples:
- Could spoof (ie. appear to be sent from) **Serve Help Desk serve@gcsu.edu**
- Could be sent from **GC President president@gcsu.edu**
- Could be sent from companies **Amazon Support support@amazon.com**
- Could be spoofing an individual **Hance Patrick hance.patrick@gcsu.edu**

EMAILING IMAGES

- Stealing images from legitimate websites is easy
- Imbedding images and delivering them through email is also easy to do

HOW TO TELL IF AN EMAIL IS LEGITIMATE

- TECHNICALLY IT'S VERY HARD IF NOT IMPOSSIBLE TO DETERMINE THAT AN EMAIL IS 100% LEGITIMATE
- KNOW THAT EMAIL IS NOT A SECURE NOR GUARANTEED COMMUNICATION
- EVERY EMAIL: DETERMINE CONTEXT AND PLAUSIBILITY
- KNOW HACKERS TECHNIQUES
- NEVER CLICK ON URL'S PROVIDED IN EMAILS THAT YOU DIDN'T EXPECT

PHISHER/HACKER TECHNIQUES

- TRY TO GAIN YOUR CONFIDENCE BY REPRESENTING THEMSELVES AS LEGITIMATE
- THEY PRESENT A SITUATION THAT EITHER SIMULATES REALITY (TO GAIN TRUST) OR CAUSES YOU TO PANIC
- THEY WANT YOU TO CLICK ON THE URL OR OPEN THE ATTACHMENT
- THE CONTENT AT THE URL MAY LOOK REAL
- THEY ARE EITHER STEALING YOUR INFORMATION, LOADING A VIRUS, OR BOTH

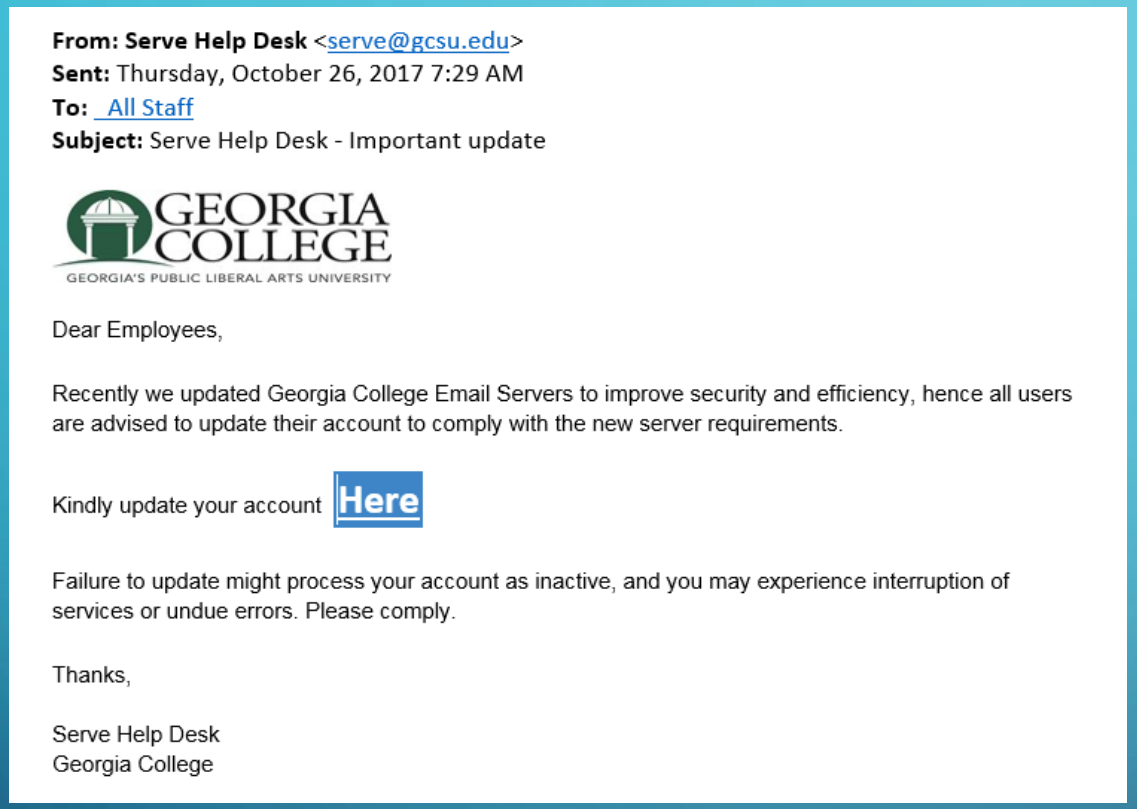
PHISHING RESULTS

- BY FALLING FOR A FAKE ADP EMAIL, MANY USG EMPLOYEES HAD THEIR PAYCHECKS DIRECT DEPOSITED TO THIEVES
- MANY GCSU STUDENTS, FACULTY AND STAFF HAVE HAD THEIR EMAILS DISRUPTED BY PROVIDING THEIR GCSU CREDENTIALS TO HACKERS POSING AS SERVE
- MANY PEOPLE ACROSS THE U.S.A. HAVE HAD THEIR BANK ACCOUNTS DRAINED BY THIEVES POSING AS THEIR BANK
- MANY PEOPLE ACROSS THE U.S.A. HAVE HAD THEIR CREDIT CARDS STOLEN BY PROVIDING THIEVES THEIR CREDENTIALS TO MISCELLANEOUS ACCOUNTS
- MANY COMPANIES AND UNIVERSITIES HAVE WIRED MONEY TO THEIVES POSING AS PRESIDENTS, OFFICERS, AND SOMETIMES VENDORS

WHAT TO DO?

- DON'T CLICK ON HIDDEN URL'S (BUTTONS, CLICK HERE MESSAGES, ETC.)
- BE WARY OF THE URL'S PROVIDED (THEY CAN BE MASKED/FAKED)
- TYPE THE URL BY HAND, OR IF LONG AND YOU TRUST THE URL BEING DISPLAYED, USE CUT AND PASTE
- WHEN IN DOUBT, CALL

PHISH OR LEGITIMATE



From: Serve Help Desk <serve@gcsu.edu>
Sent: Thursday, October 26, 2017 7:29 AM
To: All Staff
Subject: Serve Help Desk - Important update

GEORGIA COLLEGE
GEORGIA'S PUBLIC LIBERAL ARTS UNIVERSITY

Dear Employees,

Recently we updated Georgia College Email Servers to improve security and efficiency, hence all users are advised to update their account to comply with the new server requirements.

Kindly update your account **Here**

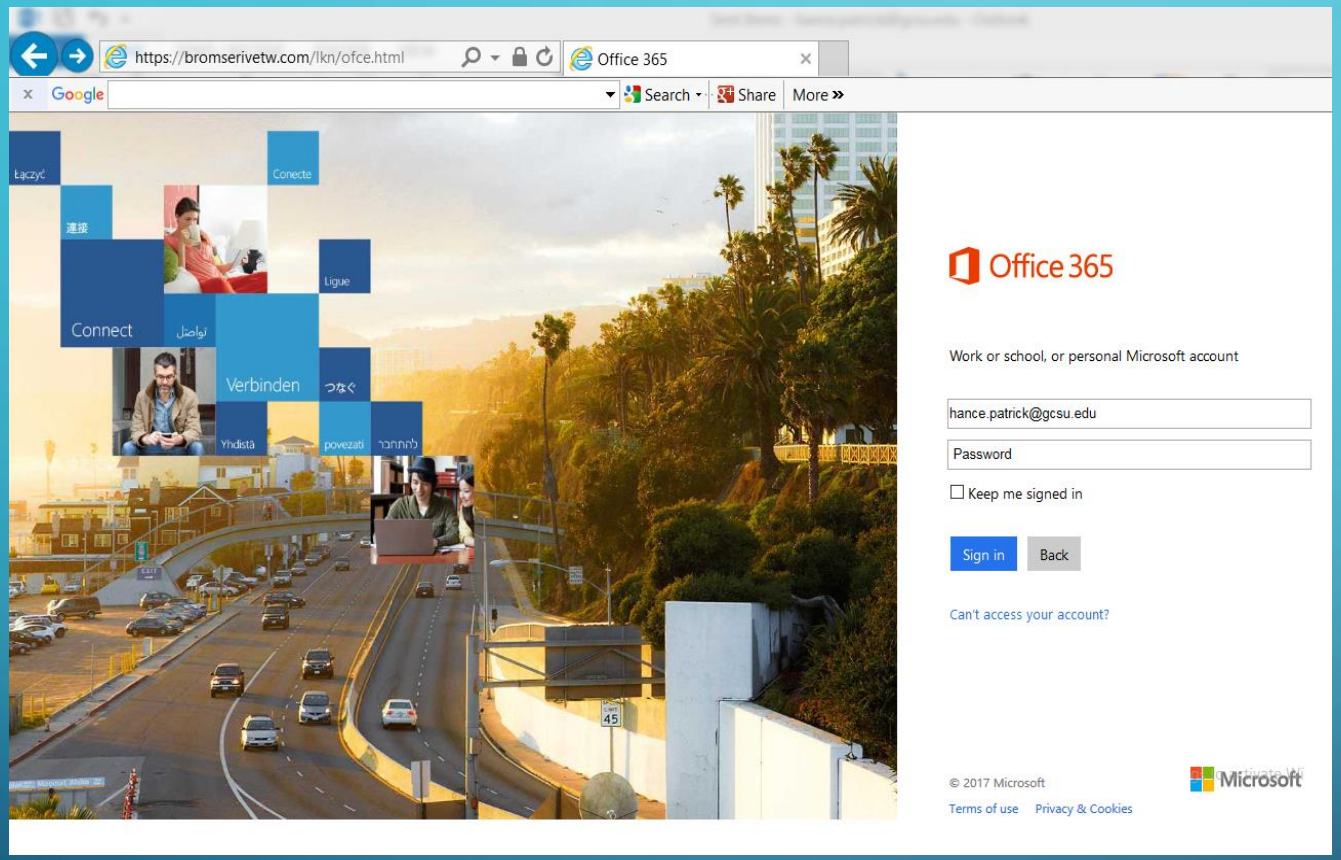
Failure to update might process your account as inactive, and you may experience interruption of services or undue errors. Please comply.

Thanks,

Serve Help Desk
Georgia College

PHISH: THE SPOOF IS DONE WELL, AND THEY USE AN ACTUAL GCSU EMBLEM. HOWEVER, THE SCENARIO IS NOT ONE THAT SERVE WILL SEND TO YOU (ie. highly implausible), AND THEY'LL NEVER PRESENT YOU WITH A "Here" BUTTON WITH A HIDDEN URL. IF EVER IN DOUBT, CALL SERVE AT x7378 OR SEND THEM AN EMAIL.

IF YOU CLICKED ON THE URL



THIS IS WHAT YOU SAW. NOTICE THAT IT'S EXACTLY THE SAME AS MICROSOFT OFFICE 365. ONCE YOU PRESSED THE SIGN IN BUTTON THEY'VE STOLEN YOUR CREDENTIALS. NOTICE THE URL.

PHISH OR LEGITIMATE

From: Serve
Sent: Tuesday, October 31, 2017 11:15 AM
Subject: Your account may have been hacked. Please contact us ASAP.

Your GCSU email account is sending out spam. It's possible that your account has been compromised or that you have a virus on your PC.

Please contact the Serve Help Desk at x7378 as soon as possible. We'll need to reset your passwords and check your machines for viruses.

Patricia
Serve Help Desk
GEORGIA COLLEGE
Campus Box 050
Milledgeville, GA 31061
Office: 478-445-7378
Serve@gcsu.edu

SERVE HELP DESK

LEGITIMATE: WHILE YOU WERE PROBABLY NOT EXPECTING THE EMAIL, THE SCENARIO IS PLAUSIBLE AND ONE THAT SERVE SHOULD CONTACT YOU. THEY ARE NOT SUPPLYING A URL, BUT PROVIDING THEIR PHONE NUMBER. IF EVER IN DOUBT, CALL SERVE AT x7378 OR SEND THEM AN EMAIL.

PHISH OR LEGITIMATE

From: Steve Dorman <steve.dorman@gcsu.edu>
CC: <steve.dorman@gcsu.edu> [mailto:gausemus@usd250.org]
Sent: Friday, October 28, 2017 11:08 AM
Subject: Payment

Hi Omega,

Are you available in the office? I need you to complete a payment today for $25,200.

I will send you beneficiary bank info soon. Kindly confirm receipt of my email.

Regards,

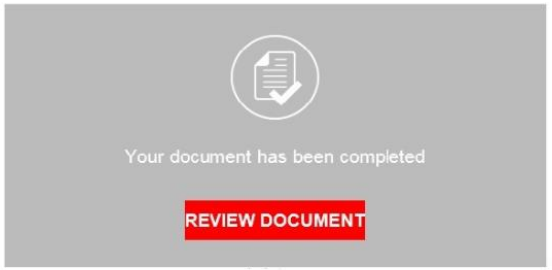
Steve

PHISH: THE SPOOF IS DONE WELL, BUT THERE IS AN INTERESTING EMAIL CC'd. IT WAS SENT TO ACCOUNTING, BUT IS ASKING THEM TO BYPASS THEIR PROCEDURES AND IN A LATER EMAIL ASKS THEM TO WIRE TRANSFER THE MONEY. NEVER BYPASS YOUR PROCEDURES! IF IN DOUBT, CALL THE PERSON.

PHISH OR LEGITIMATE

PHISH:

From: Cameron Smith via DocuSign <dse@docusgn.com>
Subject: Completed: gcsu.edu - Wire Transfer Instructions for Document
Reply-To: Cameron Smith via DocuSign <dse@docusgn.com>



All parties have completed gcsu.edu - Wire Transfer Instructions for Document Ready for Signature.

Please review and sign your Wire Transfer Instructions for

via DocuSign by clicking on the "Review Document" button above. Signing will not be complete until you have reviewed the agreement and confirmed your signature. Please make sure to fill out the TaxID if you are requesting for credit terms. Please let us know if you have any questions. Thank you.

Powered by DocuSign

ACTUAL:

From: "GC Signatures via DocuSign" <dse_demo@docusign.net>
Subject: COAS Proposal of New Undergraduate Course for .0 010
Reply-To: GC Signatures <gcsignature@gcsu.edu>

GC Signatures
gcsignature@gcsu.edu

A COAS Proposal of New Undergraduate Course has been submitted for your review and / or approval. There are several processing steps and approvals involved in this review. When all reviews have been completed, copies will be sent to the appropriate recipients. If you wish to check on the progress of this document, simply open your original e-mail and click the enclosed link entitled "Review Documents".

Please contact the College of Arts & Science Dean's office at 478-445-4441 for assistance if you:
-Received this message in error.
-Are unable to view the document.
-Have questions about the document.

Powered by DocuSign

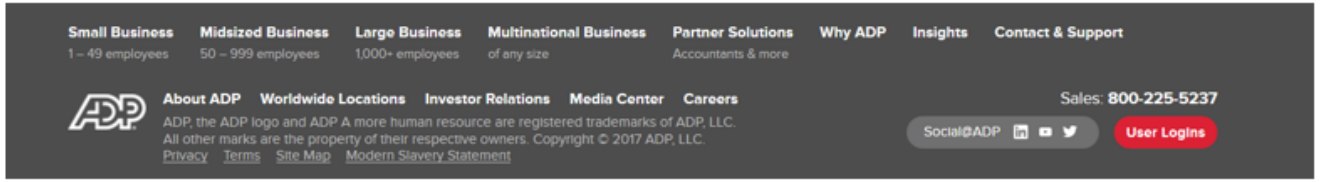
PLAUSIBLE SCENARIO BY THE PHISH, BUT THE EMAIL WAS UNEXPECTED. THERE IS NO WAY TO VERIFY IT. ON THE RIGHT IS THE ACTUAL EMAIL, WITH NUMBERS TO CALL FOR VERIFICATION.

PHISH OR LEGITIMATE

From: ADP Customer Support customersupport@adp.com
Date: October 9, 2017
Subject: Verify your ADP Account

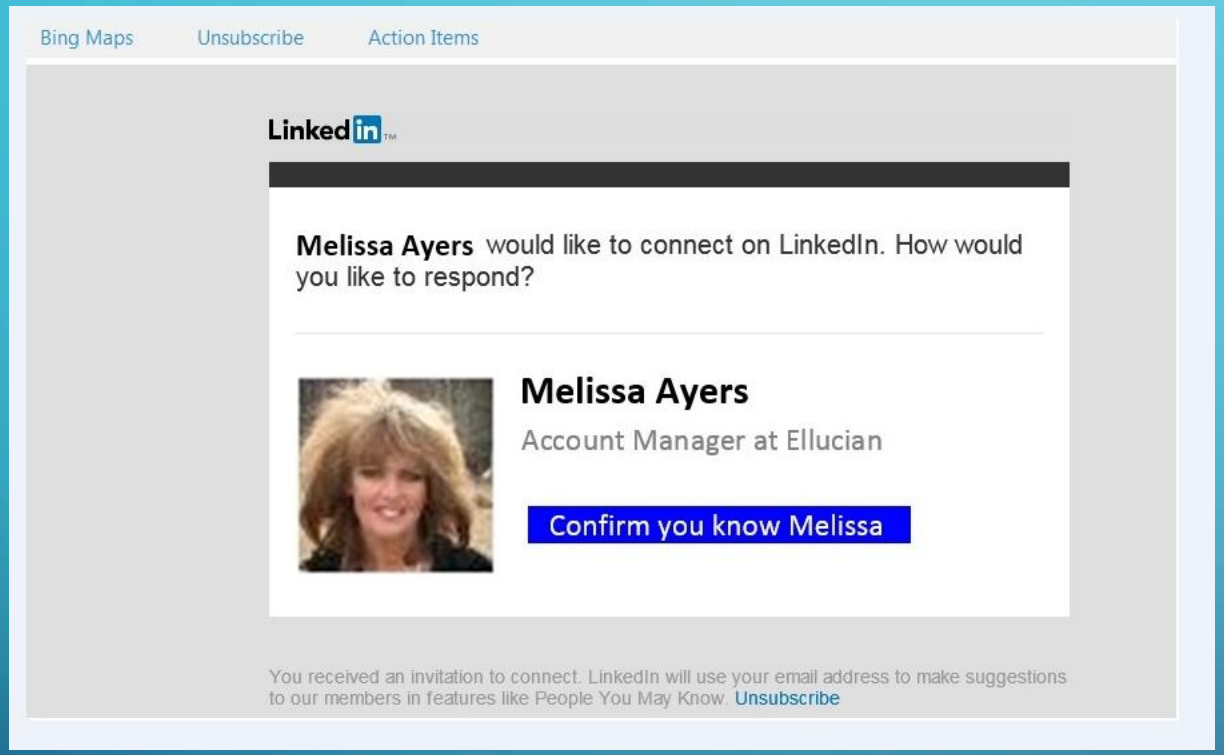
We've noticed that some of your account information appears to be missing or incorrect, we need to verify your account information in order to continue receiving your payroll checks.

Please verify your account by clicking on the link below. Sign in user your ADP user account and password. **Verify Now.**



PHISH: THE SPOOF IS DONE WELL, BUT ADP WILL NEVER HAVE YOU "VERIFY YOUR ACCOUNT". THE HIDDEN URL TOOK PEOPLE TO A SITE THAT HAD STOLEN THE ADP LOGIN PAGE. WHEN PEOPLE PROVIDED THEIR ADP INFORMATION CRIMINALS CHANGED THEIR DIRECT DEPOSIT TO GO OVERSEAS.

PHISH OR LEGITIMATE



PHISH: NEVER CLICK ON A HIDDEN URL (THIS ONE HIDDEN UNDER "Confirm you know Melissa"). THIS ACTUALLY TAKES YOU TO ANOTHER URL NOT ASSOCIATED WITH Linkedin BUT LOOKS EXACTLY LIKE THEIR LOGIN PAGE. THEY'RE STEALING YOUR ACCOUNT NAMES AND PASSWORDS. OFTEN THEY USE THIS TO TRY TO LOG IN TO OTHER SITES.

PHISH OR LEGITIMATE

Microsoft account

Microsoft

Unusual sign-in activity

Someone recently used your password to try to sign in to your Account.

We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please see below sign-in details:

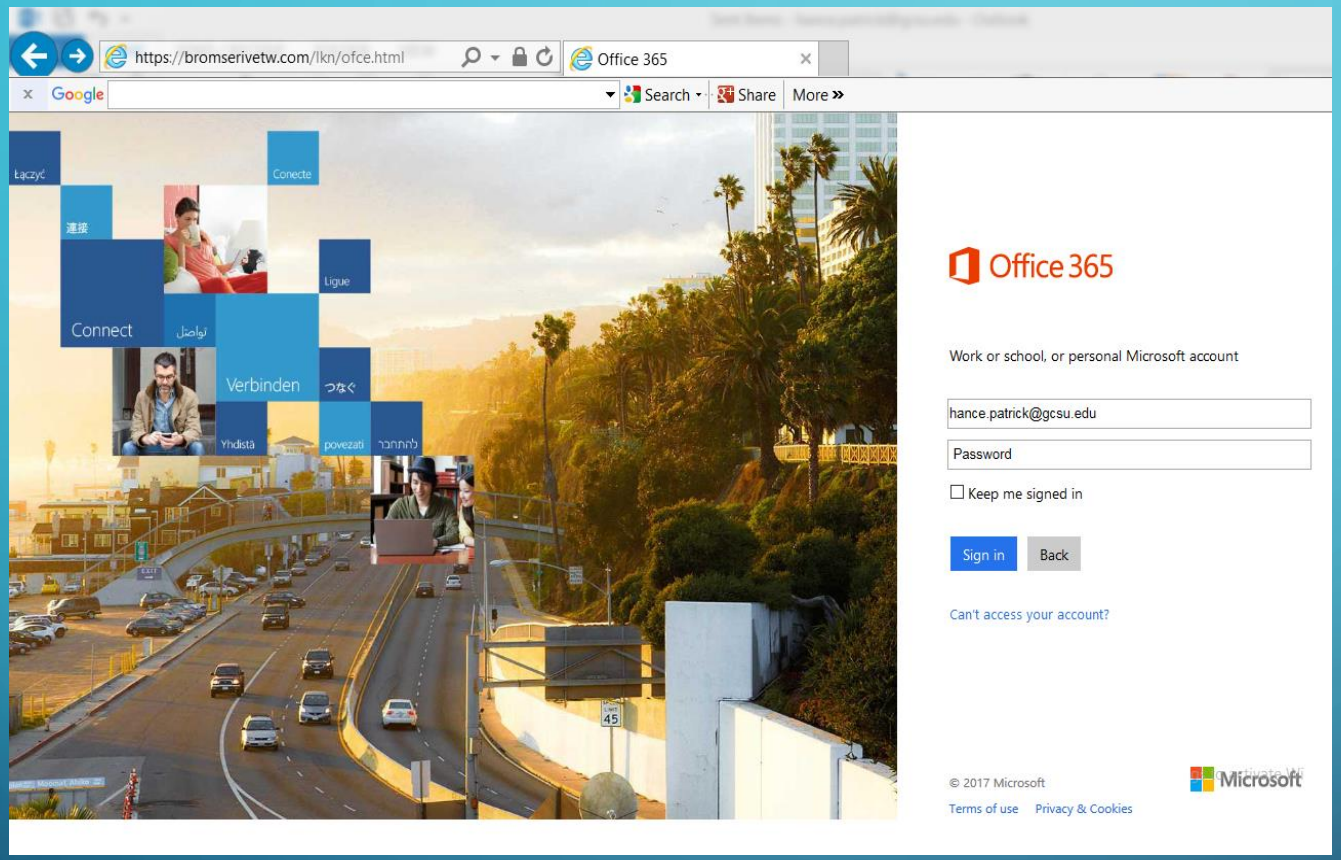
IP Address: 24.89.41.233
Location: WINHOEK, NAMIBIA

If this is not from your account, please click here to verify your account.

The Microsoft team

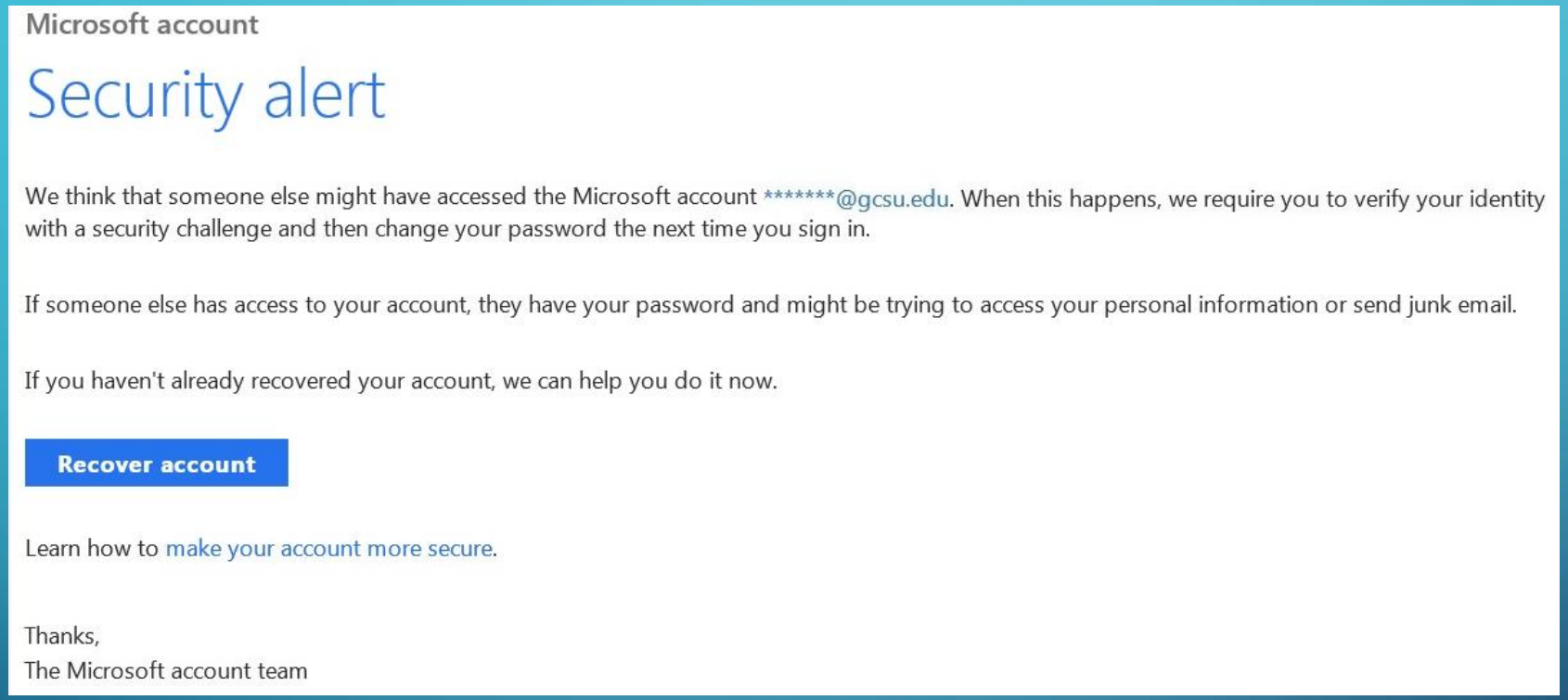
PHISH: THE SPOOF IS NOT ACCURATE BUT PLAUSIBLE, AND THE SCENARIO IS PLAUSIBLE RIGHT UP UNTIL THE “please click here to verify your account.” DO NOT CLICK ON HIDDEN URL’s. MICROSOFT WILL NOT ASK YOU TO DO THIS. THIS IS A CLASSIC PHISH.

IF YOU CLICKED ON THE URL



THIS IS WHAT YOU SAW. NOTICE THAT IT'S EXACTLY THE SAME AS MICROSOFT OFFICE 365. ONCE YOU PRESSED THE SIGN IN BUTTON THEY'VE STOLEN YOUR CREDENTIALS. NOTICE THE URL.

PHISH OR LEGITIMATE



Microsoft account

Security alert

We think that someone else might have accessed the Microsoft account *******@gcsu.edu. When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now.

Recover account

Learn how to make your account more secure.

Thanks,
The Microsoft account team

PHISH: THE SCENARIO IS PLAUSIBLE RIGHT UP UNTIL THE “Recover account” BUTTON. DO NOT CLICK ON HIDDEN URL’S. MICROSOFT WILL NOT ASK YOU TO DO THIS. THIS IS ANOTHER CLASSIC PHISH.

PHISH OR LEGITIMATE

From: Amazon.com Reviews <customer-reviews-messages@amazon.com>
Sent: Thursday, March 30, 2017 1:02 PM
Subject: Did 'Klipsch RP-280-FA Home Theater System Bun...' meet your expectations? Review it on Amazon.com

amazon.com.

How did this item meet your expectations?

Klipsch RP-280FA Home Theater System Bundle (Black) with Yamaha RX-A2050
by Klipsch
$4,619^{00}

Start by rating it

☆ ☆ ☆ ☆ ☆

If this email was sent to you in error, please click here to report this to Amazon technical services.

PHISH: PERFECT SPOOF AND PERFECT SCENARIO. THEY USE ACTUAL EMAILS AND ACTUAL IMAGES, AND IF YOU PANIC BECAUSE YOU KNOW YOU DIDN'T PURCHASE A $4,619 HOME THEATER SYSTEM, THEY SEND YOU TO A SITE WHERE THEY'VE STOLEN THE AMAZON LOGIN PAGE. THEY'RE ACTUALLY STEALING YOUR CREDENTIALS TO STEAL YOUR CREDIT CARD.

PHISH OR LEGITIMATE

From: Account Support <support@bankofamerica.com>
Sent: Tuesday, October 31, 2017 1:21 PM
Subject: Your account is overdrawn

Bank of America

At this time your account is overdrawn. Please log in to review recent activity and to deposit more funds into your account.

Bank of America
Account Support

PHISH: THEY WANT YOU TO PANIC AND CLICK ON THE "log in", WHERE THEY HAVE A LOGIN PAGE THAT LOOKS LIKE BANK OF AMERICA. IT'S EASY TO DO. ONCE YOU THINK YOU'RE LOGGED IN THERE IS NO UNUSUAL ACTIVITY SO YOU JUST EXIT. MEANWHILE IN A FEW MINUTES THE CRIMINAL USES YOUR CREDENTIALS TO DRAIN YOUR ACCOUNT.

PHISH OR LEGITIMATE

From: Kelly Prior [mailto:kelly.prior@gcsu.edu]
Sent: Tuesday, October 31, 2017 1:31 PM
Subject: Annual Employee Compliance Training

Good Morning,

Once again it is time to complete the required Annual Employee Compliance Training at Georgia College. The training is a University System of Georgia requirement for all employees (faculty, staff and student workers). This year's content consist of institutional and system policies and procedures, information and data security and Motor Vehicle Use. All employees, including student workers, must complete the *Policy Compliance and Ethics Refresher* and *Information Security Awareness module*. Individuals who drive on university business must also complete the *Motor Vehicle Use Program module*.

Please see the information below on how to access and complete the training.

Accessing the Training:

- Login to Unify at https://unify.gcsu.edu

- Click on GeorgiaVIEW and access using your Unify credentials (third icon under the OneUSG Connect Information)

- In the "My Courses" section, click on "2017 Required Annual Training" or you can click the "Select a Course" dropdown in the top right section of the screen and select "2017 Required Annual Training"

LEGITIMATE: THE EMAIL LOOKS LIKE A GCSU.EDU EMAIL, IT COMES FROM AN H/R EMPLOYEE, AND THE SCENARIO IS ACCURATE AND TIMELY. THE URL ISN'T HIDDEN, BUT IF WE WEREN'T CERTAIN WE COULD ALWAYS GO TO UNIFY BY HAND. IF YOU'RE IN DOUBT, I'M SURE THAT KELLY WOULDN'T MIND ANSWERING YOUR PHONE CALL.

PHISH OR LEGITIMATE

From: Cyndi E Johnson [mailto:cynthia.johnson@gcsu.edu]
Sent: Tuesday, October 31, 2017 1:39 PM
Subject: GC Required Course - Haven for Faculty and Staff

Dear Faculty and Staff,

Based upon the new USG Sexual Misconduct Policy (effective July 1, 2016), every employee at GC is required to participate in the Haven (from EverFi) training. USG institutions have partnered with EverFi to deliver online education on sexual harassment, connect you with support resources, discuss factors that contribute to sexual and relationship violence and empower you to become a leader in prevention.

Prevention is one of the primary mechanisms used to reduce incidents of sexual violence on campuses. USG institutions are required to provide prevention tools and to conduct ongoing awareness and prevention programming and training for the campus community including students, faculty, and staff.

Please complete Part 1 of Haven for Faculty and Staff **before September 30, 2016**. After 30 days you will receive an invitation to complete Part 2 of Haven for Faculty and Staff which must be completed by November 11, 2016.

INSTRUCTIONS:

1. Log in to Unify: https://unify.gcsu.edu/
2. Click on the "PAWS" button in the middle of the page.
    - When entering PAWS, if "PERSONAL INFORMATION REVIEW" appears you must enter the required fields and submit before you can proceed.
3. Click on "Haven for Faculty and Staff" from the Main Menu.
4. You will then have to click on the link (button) that will take you to a secure EverFi site where you will access the courses.

LEGITIMATE: WHILE YOU WEREN'T EXPECTING THIS EMAIL, THE SCENARIO IS PLAUSIBLE. IN THIS CASE THE EMAIL ADDRESS IS SPOOFED BECAUSE CYNDI DIDN'T SEND THE EMAIL, BUT SHE DOES WANT TO RECEIVE ANY REPLIES. THE URL'S ARENT HIDDEN AND YOU CAN TYPE THEM BY HAND. I'M SURE THAT CYNDI WOULDN'T MIND ANSWERING YOUR PHONE CALL.

EXAMPLES OF RECENT PHISH BEING CIRCULATED

- **Subject: Google Doc Phishing Message**
- What appears to be a wide-spread Internet worm hit the campus in the form of a phishing email message. The message slipped through normal spam filters as the worm virus spread to email accounts in the "bobcats.gcsu.edu" domain.
- **Subject: Message from payroll**
- This message, appearing to come from the Payroll department, was successful at convincing several campus recipients to click on the link provided and enter their ADP credentials. The link was directed to a fake ADP login page, the account name and password entered on this page would be compromised.
- **Subject: Serve Help Desk – Important update**
- This is an example of how phishing messages can be made to look like they are from Georgia College, such as the Serve Help Desk. GCSU images were used as well as the email was spoofed. If users clicked through they were provided a page that simulated Office365 where they provided their Unify/Email credentials.
- **Subject: Library Account**
- This phishing message was received by students across campus, purporting that the student's library account has expired. The Library does not issue emails concerning inactive accounts.

EXAMPLES OF RECENT PHISH BEING CIRCULATED

- **Subject: Important Notice from ADP**
- This phishing message was received by faculty and staff across campus. If clicked on, the URL presented a login page that looked like ADP where credential were stolen. The criminals in this case changed peoples direct deposit to route paychecks directly to the criminals U.S. bank account where they'd then wire the monies from one account to another account overseas.
- **Subject: PO 0116366 – Placing an Order**
- A recent spate of phishing/virus messages have been received on campus purporting to have a Purchase Order attached and try to have the user open the attachment either out of curiosity or trying to convince them it's legitimate. The attachment, if opened delivered a virus.
- **Subject: Your Dropbox File**
- A recent spate of phishing messages have been received on campus purporting to be Dropbox notifications. The link in the email message to "View File" is a ruse to capture Unify passphrase credentials.
- **Subject: Download your W2**
- This was the first tax season related phishing message reported on campus this year. Beware of phishing messages containing fake instructions for downloading your W2 form.

EXAMPLES OF RECENT PHISH BEING CIRCULATED

- **Subject: FedEx Shipment Update**
- This very simple phishing message that appeared to be sent from FedEx was effective in convincing several campus recipients to download the PDF attachment. The file contained a link that required password authentication, allowing the attacker to capture these credentials for future use.
- **Subject: Irregular Activity**
- This phishing message, purportedly from Bank of America, contained multiple threats - two file attachments that likely contain malware and a separate ploy to obtain user credentials.
- **Subject: Vital Info**
- Another targeted phishing message, this one has been spoofed to appear to come from the Office of the Registrar.
- **Subject: PayPal - We need your help**
- This is an example of how phishing messages can be made to look like they are from a legitimate business, such as PayPal. However, the poor grammar and other indicators make this an easy phish to spot.

EXAMPLES OF RECENT PHISH BEING CIRCULATED

- **Subject: Last Reminder You Must Update Your Apple Account Information!**
- An email message purporting to be from Apple Support, requesting that the recipient verify their account information, has been seen in several variations on campus.
- **Subject: Help Desk Notice**
- This phish is an example of how poorly most culprits have taken steps to disguise the message - it is often the case that phishing messages are originally drafted for another school or school district.
- **Subject: Google Docs Download**
- This phish example attempts to trick the recipient into clicking on a link to a malicious website by purporting to be a link to download a Google doc.
- **Subject: ITunes Access Disabled**
- Another example of a common ploy to trick the recipient into clicking a link to a malicious website by claiming access to ITunes has been disabled.

EXAMPLES OF RECENT PHISH BEING CIRCULATED

- **Subject: IT-Service Help Desk "Password Update"**
- Another example of a phish that attempts to trick the user to click on a link to a malicious website by claiming their password will expire otherwise. This one purports to come from the IT-Service Help Desk.
- **Subject: IRS Service "Important Update"**
- The 2017 tax filing season is upon us, beware of messages requesting personal information to be updated online to make your "refund easier".
- **Subject: Paperless W2**
- Several people on campus fell for this phish, which directed the recipient to a fake ADP login page where credentials were stolen. Beware of tax related phishing exploits, like this one, during this time of year.
- **Subject: Email Account Upgrade**
- A pretty convincing phishing message that appears to come from Serve issuing a warning that the user's ID may have been compromised.

KNOW IT'S LEGITIMATE

- IF YOU DO NOT KNOW THE SENDER, IT'S POSSIBLE IT'S A PHISH
- IF YOU DO KNOW THE SENDER BUT THE SCENARIO DOESN'T "FIT", IT'S VERY POSSIBLE IT'S A PHISH (THEIR ACCOUNT COULD HAVE BEEN HACKED OR IT COULD BE SPOOFED)
- IF THE SCENARIO INCITES PANIC, IT'S VERY POSSIBLE THAT IT'S A PHISH IF THEY WANT YOU TO CLICK ON SOMETHING
- PLAUSIBLE OR NOT, DON'T CLICK ON HIDDEN URL'S IF YOU'RE NOT EXPECTING THE EMAIL
- WHEN IN DOUBT, VERIFY!!!! CALL THE SENDER. LOGIN TO YOUR ACCOUNT BY HAND.

ANTI-PHISH TIPS:

- **NEVER SEND PASSWORDS IN EMAIL**
- **THE TRAP:** You receive an urgent email that appears to be from GCSU-IT or Serve asking you to reply with your password because your account is "compromised" or "over quota" or "suspended due to inactivity".
- **YOUR DEFENSE:** GCSU and organizations that care about the protection of your information should never ask you to send bank account numbers, Social Security Numbers, driver's license numbers, health information, or health insurance information via email. Decline requests to send this information in email.
- **Remember:** Only you can protect your passphrase! Not sure if it's a phish? Drop us a line at **serve@gcsu.edu or call 478 445-7378.**
- **DON'T CLICK UNEXPECTED LINKS**
- **THE TRAP:** You receive an unexpected email that claims to be from the "Help Desk" or someone you know. It says it's urgent. You must click a link to prevent problems with your account. You may be asked to "click here" to verify your account.
- **YOUR DEFENSE:** Be skeptical of any email that you aren't expecting. Password thieves may insist that immediate action is necessary and may pretend to be your friend or some other trusted entity. Don't let these tactics trick you into letting down your guard. It is very likely a scam.
- **YOUR DEFENSE:** Hover over the link (don't click!), or for a touchscreen, press and hold the link (don't tap!) to reveal the actual URL. (Look in the bottom left corner of the browser window.) Don't click on a link unless it goes to a URL that you trust.