TEACHERS COLLEGE
COLUMBIA UNIVERSITY

Don’t Take The Bait:
How To Stay Safe From Phishing

Goals

After this section, you'll be able to:

- Define phishing
- Identify signs of a potential phishing email
- Know where to report phishing emails to and how to report them
- Understand the importance of password security

What is Phishing?

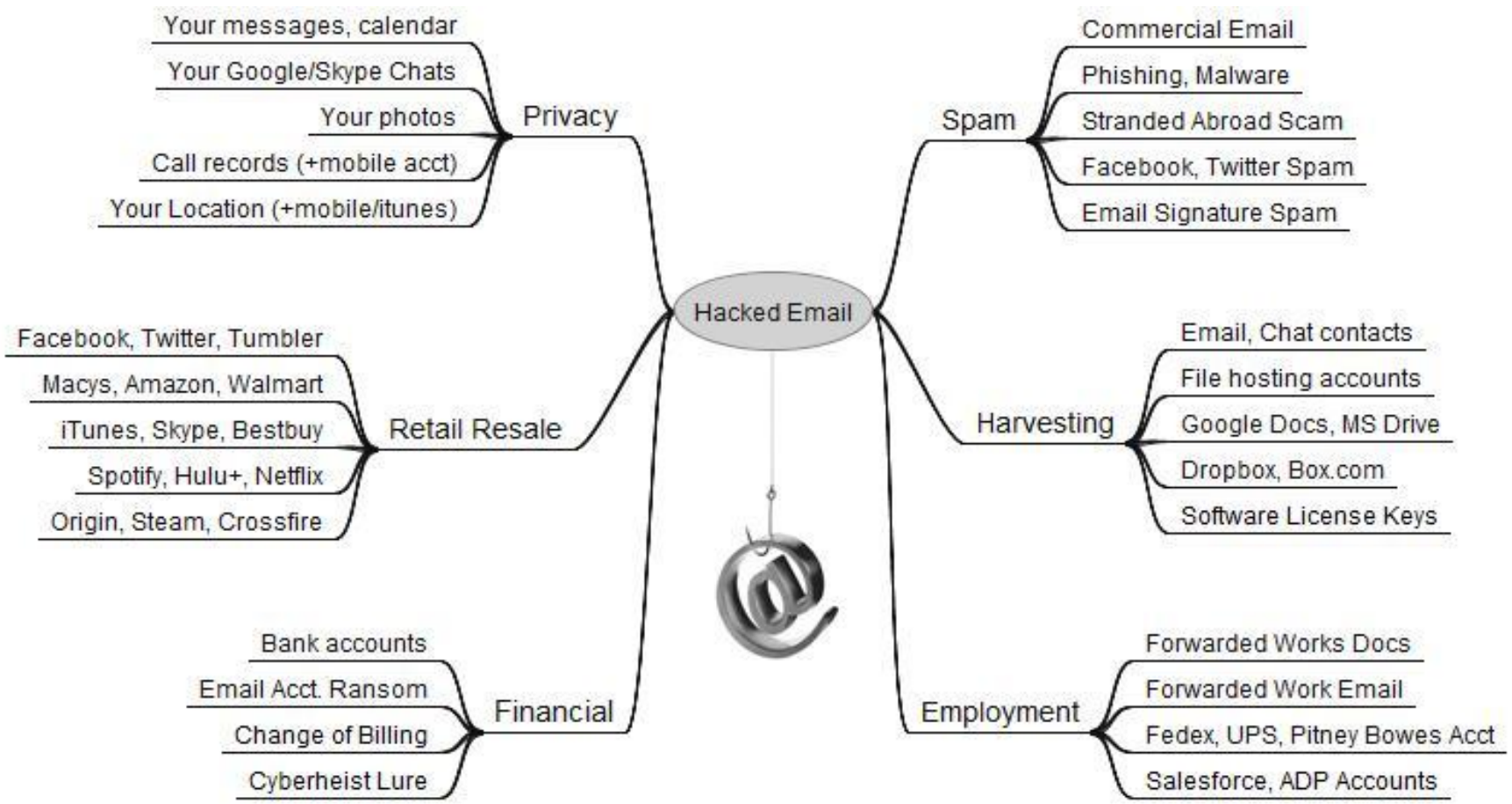
- **Phishing is a form of fraud in which the attacker tries to learn personal or financial information using social engineering**

- Two types: (1) Credential theft, (2) Download of malware
- Messages claim to be from legitimate sources
- Criminals are getting really good at creating legit-looking messages to trick people into performing actions or divulging confidential information

What Are The Risks?

- Identity Theft
- Malware infections
- Loss of personal data
- Compromised institutional information
- Putting friends and family at risk
- Financial loss

What's Your Email Worth?



Signs of A Phishing Email

- Threats/Ultimatum
- Incorrect Web addresses
- No signature or contact information
- Too-good-to-be-true offer
- Spelling, punctuation, or grammatical errors
- Attention-grabbing titles

What Does A Phishing Email Look Like?

New email scam

I do know Ireneandben1 is your pass word. Lets get directly to the point. You don't know me and you are probably thinking why you are getting this e mail? Absolutely no one has compensated me to check about you.

Let me tell you, I actually placed a malware on the xxx streaming (sexually graphic) website and you know what, you visited this web site to have fun (you know what I mean). While you were viewing video clips, your web browser began operating as a Remote Desktop with a keylogger which provided me access to your display as well as web camera. Immediately after that, my software program collected all of your contacts from your Messenger, FB, as well as e-mailaccount. Next I made a video. First part shows the video you were watching (you've got a good taste rofl), and 2nd part displays the recording of your cam, yea it is u.

You actually have a pair of choices. We are going to take a look at these types of choices in details:

Very first alternative is to skip this message. In this instance, I most certainly will send out your actual videotape to every one of your contacts and you can easily imagine concerning the shame you will definitely get. And likewise if you are in a committed relationship, just how it would affect?

Next alternative should be to compensate me $1000. Lets think of it as a donation. Consequently, I will without delay discard your video. You will go on your daily life like this never occurred and you will never hear back again from me.

You'll make the payment through Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1HgQjTregbxKLCrSThbW1YhqtuikpQRta7
[CASE-SENSITIVE so copy and paste it]

Should you are making plans for going to the cop, well, this email cannot be traced back to me. I have dealt with my steps. I am also not attempting to ask you for money a lot, I only want to be rewarded. I have a specific pixel within this email, and right now I know that you have read this e-mail. You have one day in order to pay. If I do not get the BitCoins, I will definately send your video recording to all of your contacts including close relatives, coworkers, and so on. Nevertheless, if I do get paid, I'll erase the video right away. It's a non-negotiable offer and thus don't waste my time & yours by replying to this email. If you want to have evidence, reply with Yup! and I will send out your video to your 13 contacts.

Real Phishing Email Targeting TC

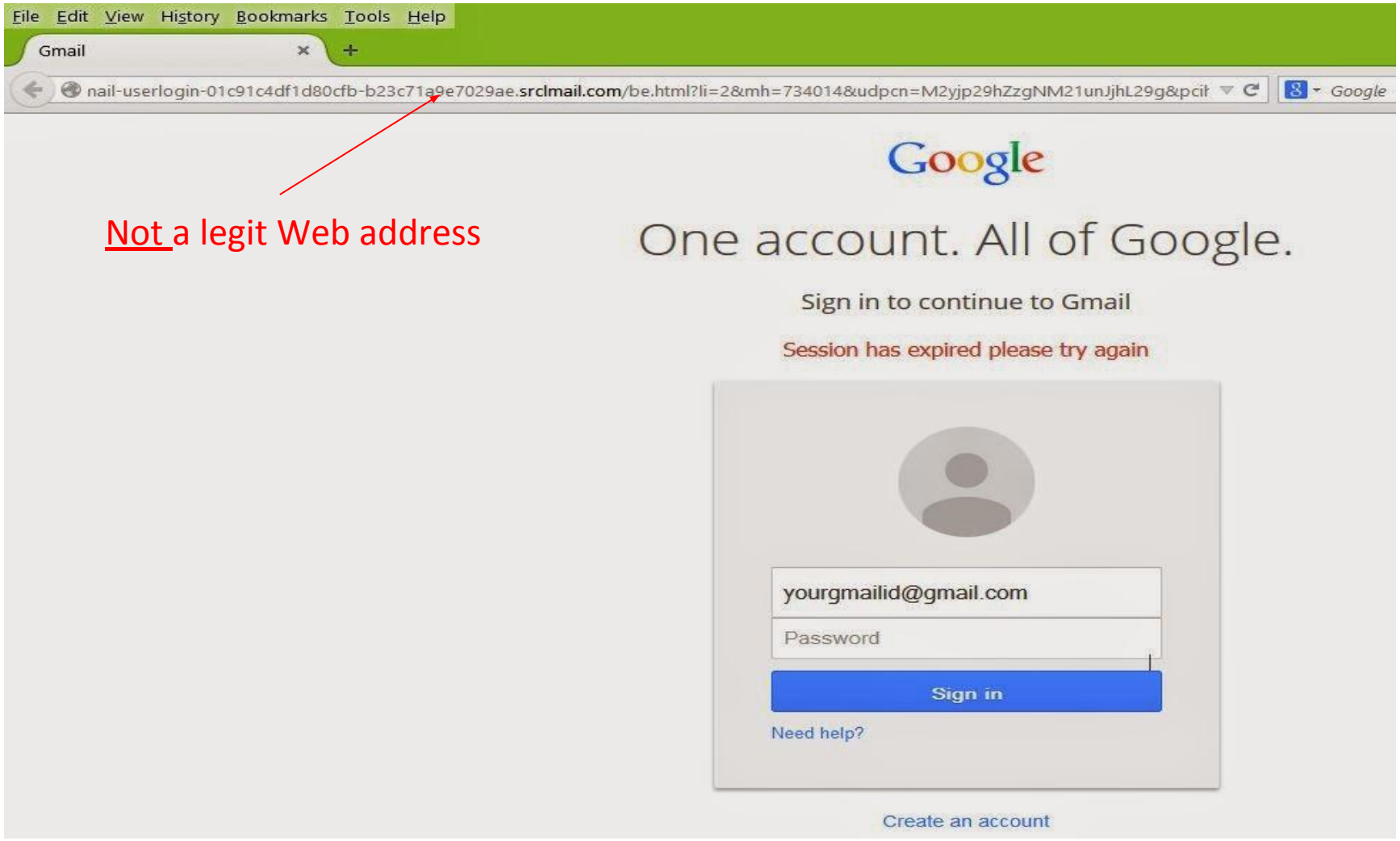
From: Faculty & Staff
Date: Sun, Mar 19, 2017 at 7:21 AM
Subject: Meeting Scheduled
To:

A meeting has been scheduled,

[Click here to view details]

Thank you
Columbia University

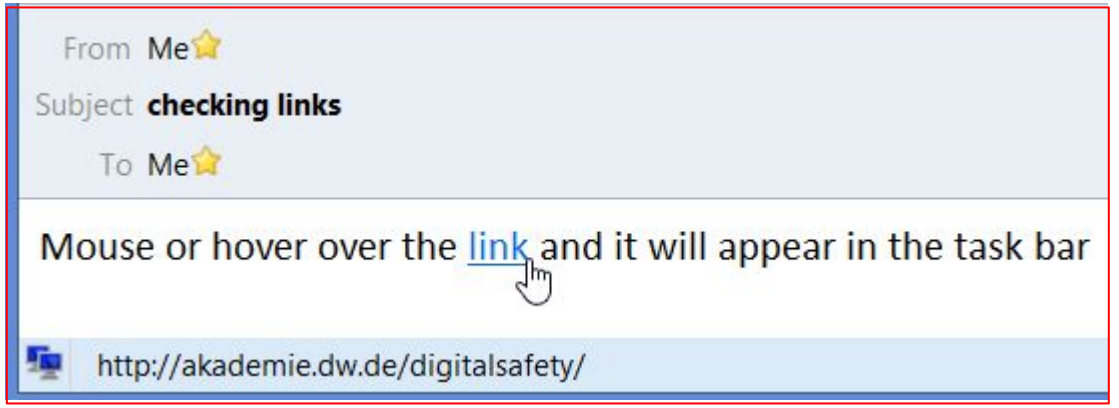
Double-Check That Login Screen



- Web address for Google login SHOULD be: accounts.google.com

What Can You Do?

- Avoid opening suspicious email attachments and following links sent in emails.



- Be mindful of emails that just don't sound right.

- When in doubt about the authenticity of an email, contact the sender via PHONE **(Do not email the sender!)**

- Forward any suspicious email to the Service Desk at servicedesk@tc.columbia.edu. You can also call the Service Desk at ext. 3300

What CIS Is Doing To Fight Phishing

On report of phishing attempts:

- We use our security tools to quickly determine how many people received the email (Agari)
- We notify all recipients of the email to alert them to not open the message or click on any links
- We block the phisher's return email addresses
- We block access from the TC network to phishing websites (OpenDNS)
- We work to tune our rules that flag phishing email as spam

What If I Clicked On The Link/Attachment?

- If taken to a login page, close the page!
- Disconnect your device from the Internet
- Backup your files
- Call the Service Desk (if this is your home computer, run your antivirus software)
- Send the “headers” of the suspicious email to servicedesk@tc.columbia.edu

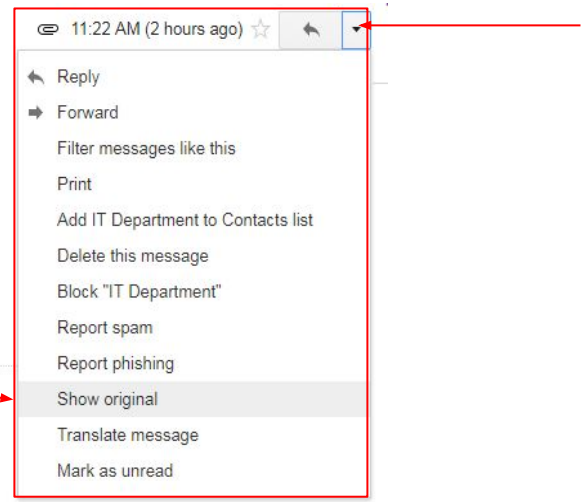
How to Download Email Headers

1. Log in to your TC Gmail account.

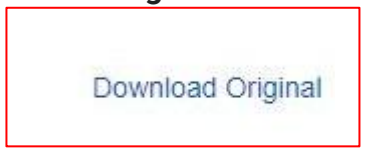
2. Open the message you'd like to view headers for.

3. Click the down arrow next to **Reply**, at the top of the message pane.

4. Select **Show Original**.



5. A summary of the headers will appear in a new window. To get the full headers, click **Download Original**.



6. Email the Service Desk at servicedesk@tc.columbia.edu and attach this file.

Tomorrow:

Workshop: “What the heck are headers?”