

WHAT THEY DO IN THE SHADOWS - UNMASKING MODERN BUSINESS SCAMS

Dr. Catherine J. Ullman
Principle Technology Architect, Security
Information Security Office
cende@buffalo.edu

 University at Buffalo
Information Technology



Agenda

- Introduction
- Social Engineering
- Old scams, new twists
- New scams
- Final Thoughts



INTRODUCTION

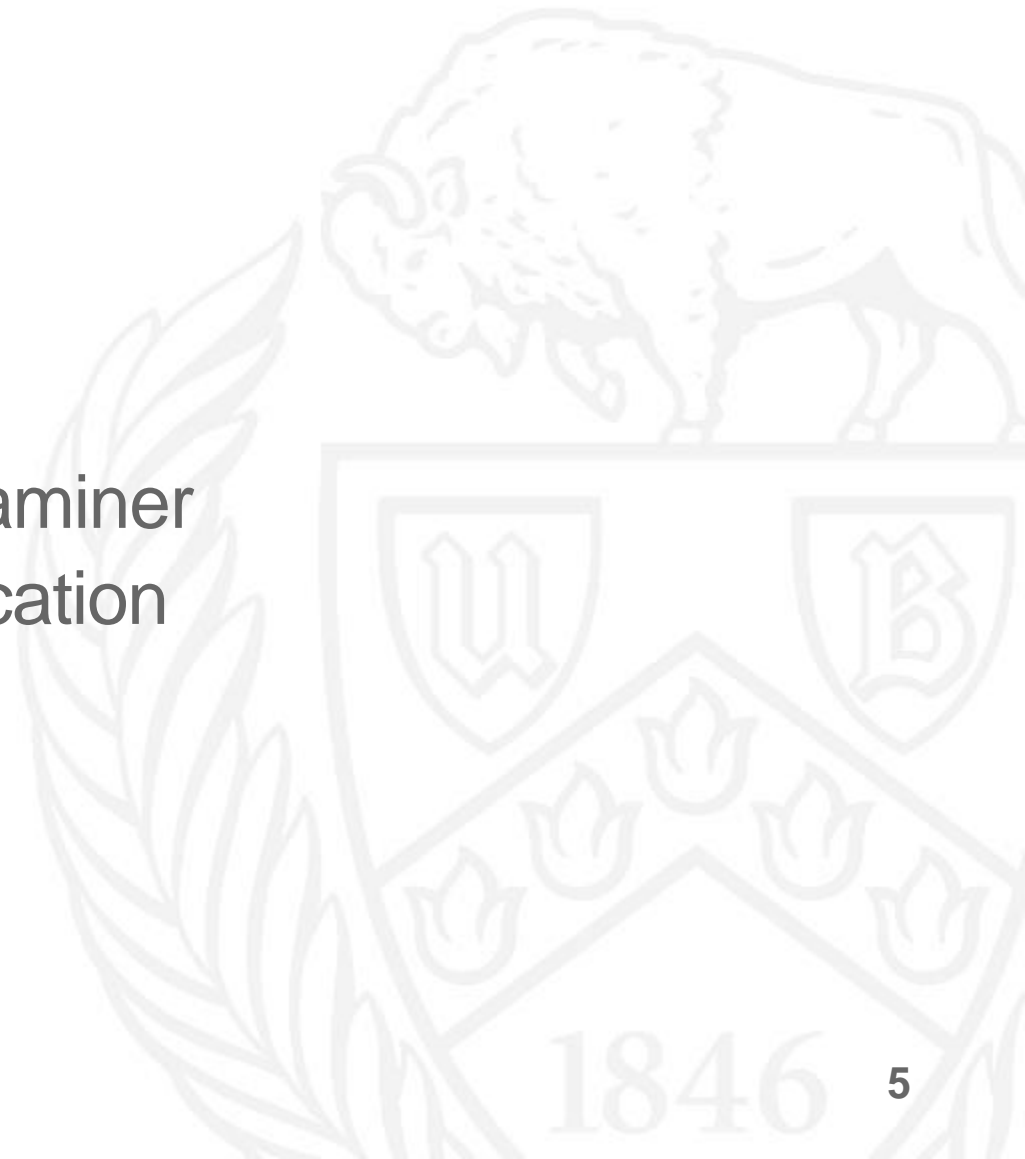


Who Am I?



But seriously...

- Principle Technology Architect, Security
- Employed at UB 23+ years
- CEH - Certified Ethical Hacker
- IACIS - Certified Forensic Computer Examiner
- GSEC- GIAC Security Essentials Certification
- MCSE, MCP+I, CNA
- M.F.S. (Master of Forensic Science)
- PhD, Philosophy



SOCIAL ENGINEERING



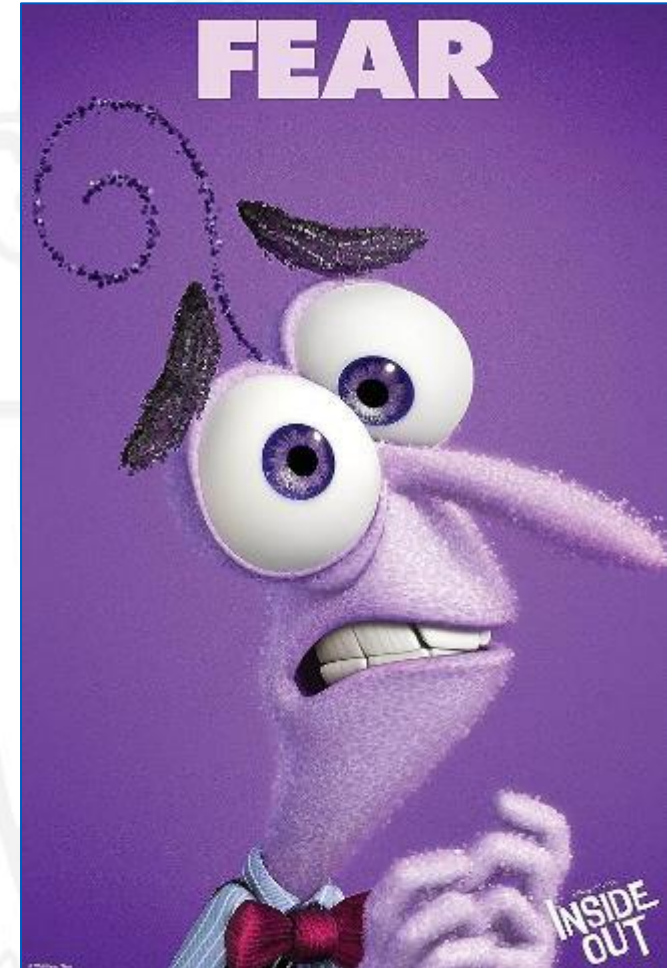
Social Engineering

“Any act that influences a person to take an action that **may or may not** be in their best interest.”



Relies on Human Nature

- Belief in others sincerity, good intentions
- Taps into primal emotions
 - Fear
 - Greed
 - Urgency



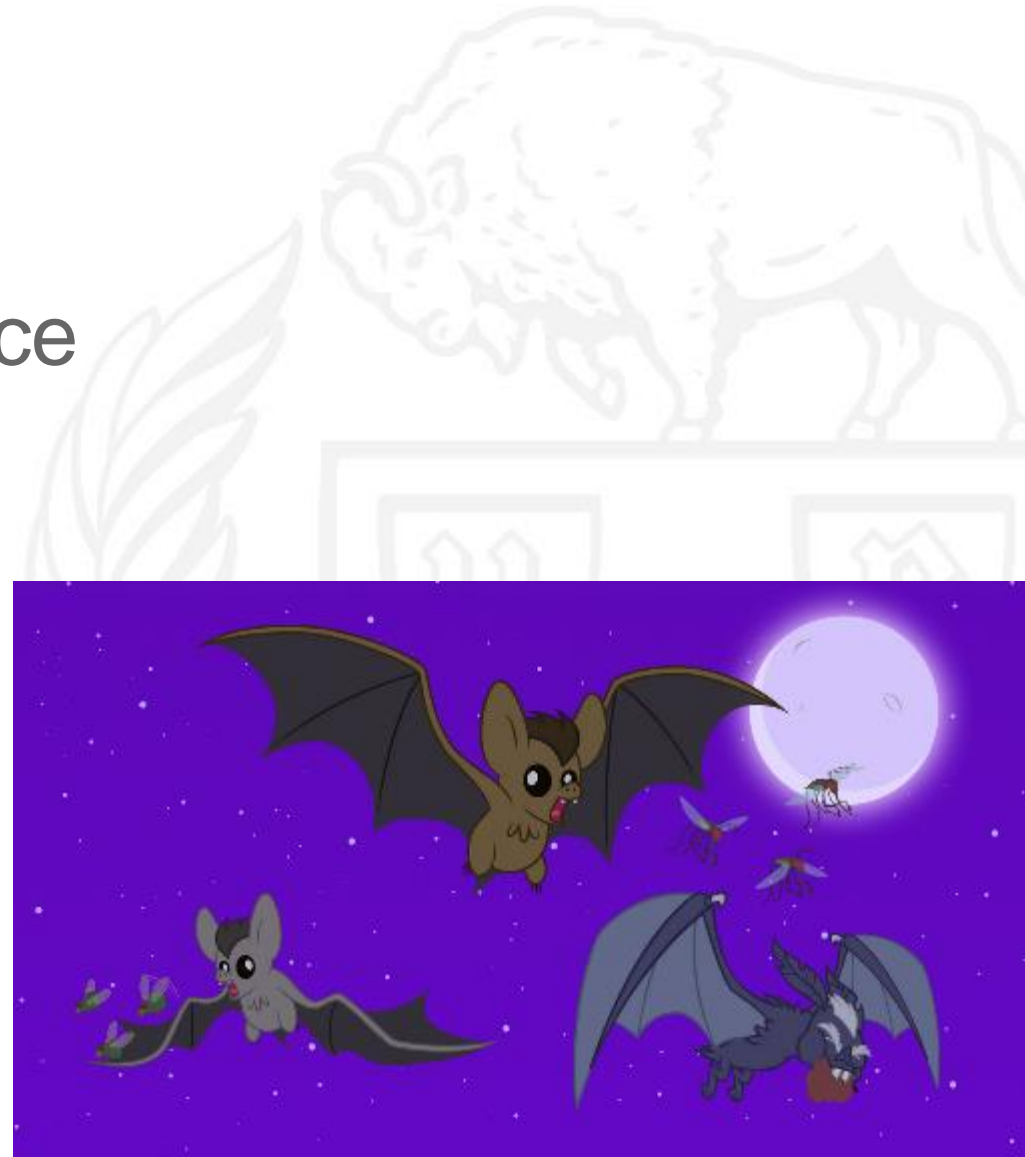
How Does Social Engineering Work?

- Information gathering
- Establish relationship
- Exploit relationship
- Attack Execution



Information Gathering

- Hunt for information via Open Source Intelligence Techniques (OSINT)
- UB websites, LinkedIn, Pastebin, Social Media



Establish Relationship

- Engage through targeted communications
 - Email
 - Phone call
 - Social media



Exploit Relationship

- Impersonate authority figure
- Friendship or liking
- Social validation
- Scarcity
- Commitment / consistency
- Social validation
- Reciprocity



Execution

- Attempt account change
 - IT, financial, health care
- Disclose sensitive information
 - Credential theft
 - Financial scam



OLD SCAMS, NEW TWISTS



Bypassing MFA – Attacker in the Middle

- Uses a proxy server
- Starts with a phishing email
- User clicks on the link and request passed to legit site
- Unlike traditional phishing, pulls content from original page
- Credentials and 2FA forwarded to attacker
- User sees successful logon

Employee “Assistance”

From: Moez Ahmed <AhmedMoe@upstate.edu>

Sent: Monday, August 28, 2023 10:14 PM

Subject: SUNY Assistance Program for Employees

Some people who received this message don't often get email from ahmedmoe@upstate.edu. [Learn why this is important](#)

This is to inform you that you are eligible to enroll in Assistance Program for employees. As an eligible employee, you are entitled to receive financial support of up to \$5,000 per applicant to assist you, your family, or any individual in need.

To enroll in the Program, you can access your application through the [SUNY Benefits Portal](#). The online registration for the Program will be available from 08/28/2023 to 09/09/2023. You are required to carefully follow all instructions provided in the Benefits Portal to submit your application successfully.

Note that all the information requested in the application is mandatory and essential for processing your application.

Sincerely,

Moez Ahmed

Employee Assistance Program

Free Stuff?

From: **Satish K Tripathi** <smitharym@gmail.com>
Date: Sat, Sep 16, 2023 at 8:22 AM
Subject: Snap - On Tools and Equipment
To:

Dear Faculty/Staff,

I hope this email finds you well. I am writing to inform you that Sharon Mitchell, Student Affairs of buffalo University , has expressed her willingness to donate her late father's Miller 951937 Dynasty 300 TIG Welder w/ TIGRunner Pkg & Wireless Foot Control, along with a complete set of Snap-On Tools and accessories.
If you are interested in any of the equipment, please indicate your interest by sending an email to sharonmitchell1467@outlook.com for a prompt response. Holder will coordinate with you to arrange inspection and delivery of the items.

Thank you for your attention and consideration.

Sincerely,

Satish K Tripathi
Email: president0@buffalo.edu
Number:(716) 6425-2901
Department: President's Office


Invoice Scams




buffalo.edu Payment-Notification: Thursday, September 14, 2023



buffalo.edu eDocument <support@merca20.com>

To Joyce Weeman

 This message was sent with High importance.
If there are problems with how this message is displayed, [click here to view it in a web browser.](#)

  Reply  Reply All  Forward 

Wed 9/13/2023 10:30 PM

1 New PDF File Received

buffalo.edu eDeposit-37478736.pdf
Payment Type: EFT | Thursday, September 14th, 2023.

[Review PDF](#)

This Transaction was successfully processed.

[Review the PDF](#)

NEW SCAMS



Generative AI Vishing

- Vishing: The practice of eliciting information or attempting to influence action via the telephone.
- AI is being used to mimic a trusted individual's voice and make requests
 - e.g. President, VP, IT Support, HR

Shared Documents (OneDrive, SharePoint, Google)

From: Julie O'Neill (via Google Drive) <drive-shares-dm-noreply@google.com>

Sent: Friday, July 28, 2023 12:03 PM

To: [<@buffalo.edu>](mailto:>@buffalo.edu)

Cc: [<@buffalo.edu>](mailto:>@buffalo.edu); [<@buffalo.edu>](mailto:>@buffalo.edu); [<@buffalo.edu>](mailto:>@buffalo.edu); [<@buffalo.edu>](mailto:>@buffalo.edu); [<@buffalo.edu>](mailto:>@buffalo.edu); [<@buffalo.edu>](mailto:>@buffalo.edu)

Subject: Document shared with you: "ASSESSED NEW PAY RISE AND BENEFIT RISE FOR ALL FACULTY AND STAFF.odt"

Julie O'Neill shared a document

Julie O'Neill (julieonell@danvers.org) has shared the following document: [Learn more](#)

FWD: Mark Alnutt, Vice President and Director of Athletics, has shared a file with you using OneDrive.

 ASSESSED NEW PAY RISE AND BENEFIT RISE FOR ALL FACULTY AND STAFF.odt

 Open

Use is subject to the Google [Privacy Policy](#).

Teams Chat Attacks

- Uses a tool that provides a fully automated attack.
- The tool verifies Teams user can receive external messages.
- Creates a new thread with the target user and sends a message with a SharePoint attachment link.
- New thread appears in the sender's Teams interface for manual interaction, ultimately initiating the attack.



MFA Fatigue

What is MFA Fatigue?

- Attacker sends MFA requests repeatedly until accepted

What actions should I take?

- Report as fraudulent
- Change your password ASAP



From: Katie Schwartz <katie@drdamonawilliams.com
<<mailto:katie@drdamonawilliams.com>> >
Sent: Thursday, April 27, 2023 10:07 AM
To: [REDACTED] <[\[REDACTED\]@buffalo.edu](mailto:[REDACTED]@buffalo.edu)> >
Cc: [REDACTED] <[\[REDACTED\]@buffalo.edu](mailto:[REDACTED]@buffalo.edu)> >;
[REDACTED] <[\[REDACTED\]@buffalo.edu](mailto:[REDACTED]@buffalo.edu)>
>; Deidra Gardner <dgardner@drdamonawilliams.com>
<<mailto:dgardner@drdamonawilliams.com>> >; [REDACTED]
<[\[REDACTED\]@buffalo.edu](mailto:[REDACTED]@buffalo.edu)> >
Subject: CSDLSI Invoice Wire Payment

Hello,

We had an issue with our Wells Fargo bank account and the wire payment was reversed; please can you confirm if you have received it back in your account?

Thank you,

Katie Schwartz

Katie Schwartz, Ph.D.

Director, Operations and Outreach

National Inclusive Excellence Leadership Academy

Center for Strategic Diversity Leadership & Social Innovation



QUESTIONS?



How did we/I do?--Take the *Session Survey* on your smart device using the QR Code on your schedule.