STAYING SAFE FROM SOCIAL ENGINEERING SCHEMES

Dr. Catherine J. Ullman
Senior Information Security Analyst
Information Security Office
cende@buffalo.edu

University at Buffalo
Information Technology

Who Am I?

But seriously…

- Senior Information Security Analyst, University at Buffalo
- Employed at UB 18+ 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


Please, may I have your password?
IHASAHOTDOG.COM BY

What is Social Engineering?

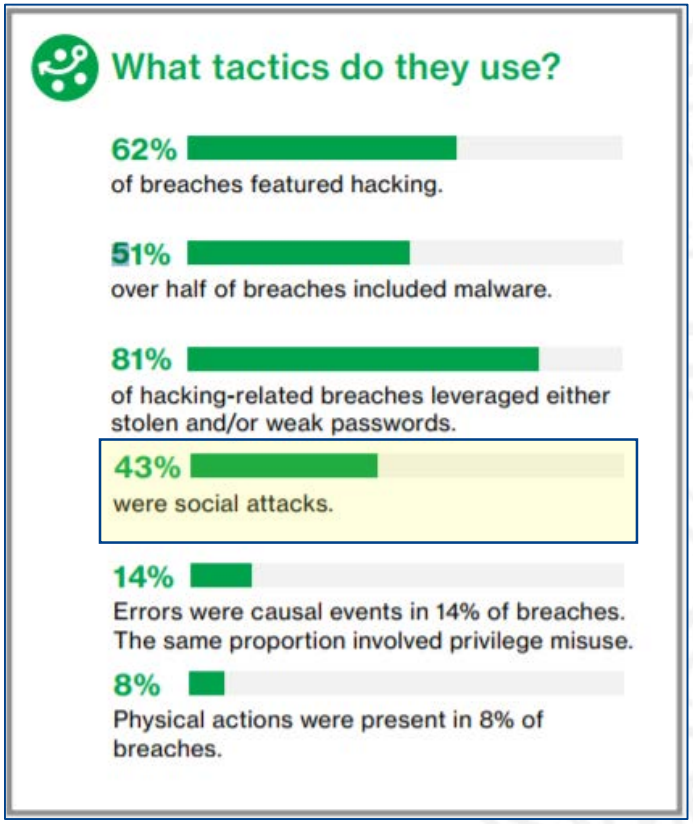
"Any act that influences a person to take an action that **may or may not** be in their best interest."

Why Social Engineering?

- Path of least resistance
  - Large return on small investment

Increased Cases of Fraud and Data Breaches

- According to the 2017 Verizon Data Breach Report, 43% of all documented breaches involved social engineering attacks.




And I should care because...?
ICANHASCHEEZBURGER.COM

Consequences - UB

- Fines
  - HIPAA - $1.5M per incident
  - NYS (SSN) – $10-$200 per SSN lost
  - PCI – Loss of ability to conduct transactions
- Lawsuits
  - Lose someone's SSN, they may sue for damages
- Overhead
  - Setup of call centers to answer questions, buying credit protection, etc

Consequences - UB

- Reputational concerns
  - faculty, students, parents, staff, granting agencies
- Growing social expectations
  - due to widespread media coverage of identity theft

Consequences - Personal

- Identity Theft
  - Thieves aren't just after the data you have access to, they're happy to take yours too!
- Financial Loss
  - Use the same password everywhere? Bad idea!
- Potential Embarrassment
  - Private information is no longer private

Some Types of Social Engineering

- Impersonation
- Vishing
- Smishing
- Phishing

Impersonation

Impersonation

- Definition?
  - "the practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system"
  - "Pretexting" is a false motive/invented scenario
- Goal?
  - Get info to compromise an organization by exploiting people's willingness to help.
  - Often pretends to need information in order to confirm the identity of the person he is talking to

Impersonation

- Examples:
  - Delivery Person (USPS, UPS, FedEx)
  - Tech Support

Vishing

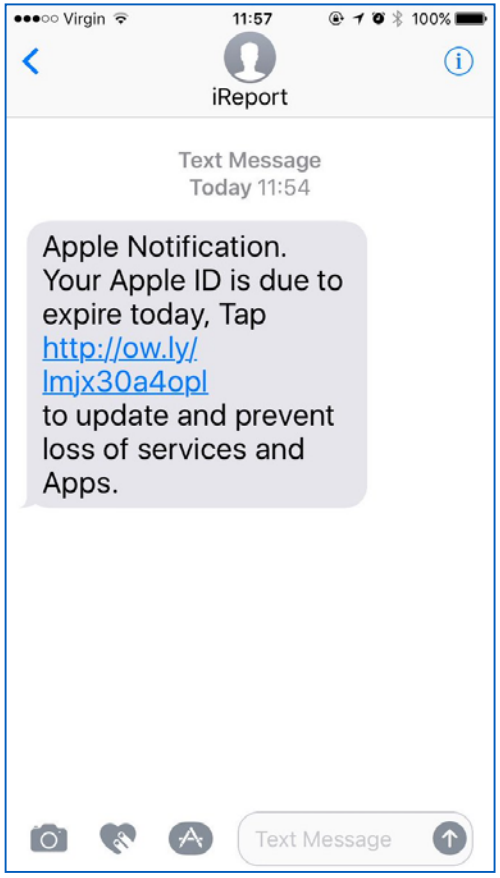
Vishing

- Definition?
  - "The practice of eliciting information or attempting to influence action via the telephone."
    - Often involves spoofed phone numbers
- Goal?
  - Get info to compromise an organization by exploiting people's willingness to help.

Vishing

- Examples:
  - Customer Support/Helpdesk Personnel (impersonate customer)
  - Tech Support (impersonate help desk)
  - Mumble Technique (mumble the answers)
  - Law Enforcement/Government Agency (FBI/IRS)

Smishing


Virgin
11:57
100%
iReport
Text Message
Today 11:54
Apple Notification. Your Apple ID is due to expire today, Tap http://ow.ly/lmjx30a4opl to update and prevent loss of services and Apps.
Text Message

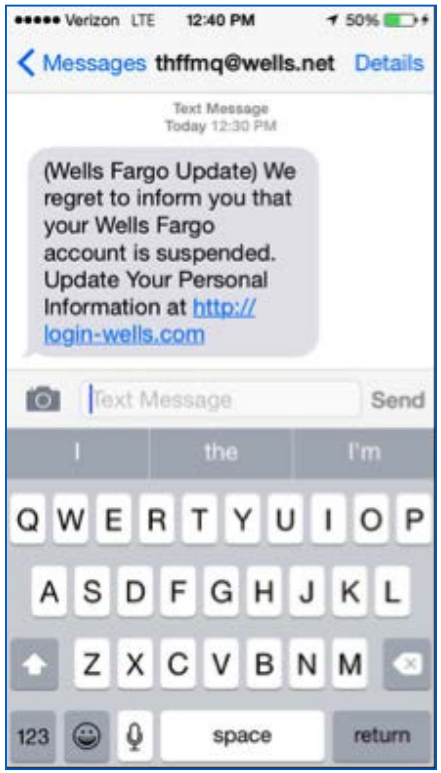
Smishing

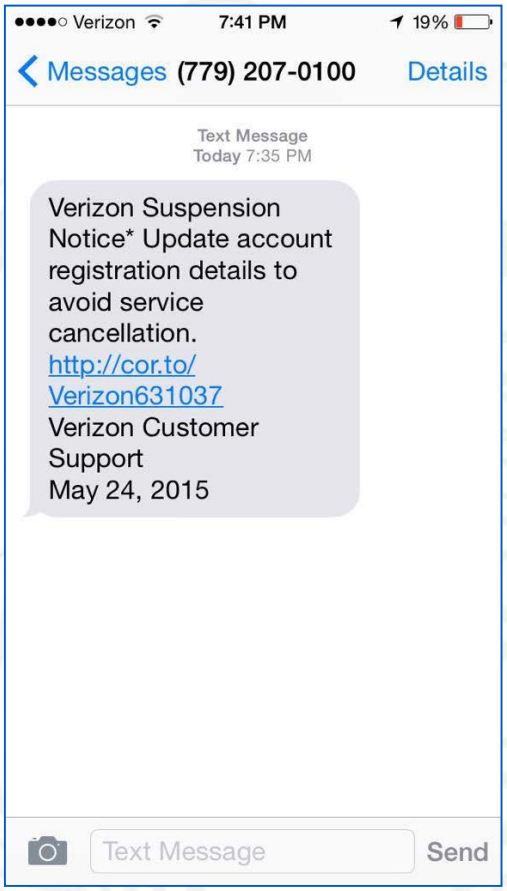
- Definition?
  - "the act of using mobile phone text messages (SMS) to lure victims into immediate action such as downloading mobile malware, visiting a malicious website or calling a fraudulent phone number"
- Goal?
  - Use fear or greed terminology to gain access to personally identifiable information or account details

Smishing

- Examples:
  - Financial Institutions (account suspended)
  - Telecommunication Companies (Verizon, AT&T, etc.)
  - Technology Companies (Apple, Microsoft)
  - Prizes/Free Gifts (movie tickets, gift cards)

Smishing Examples





Phishing

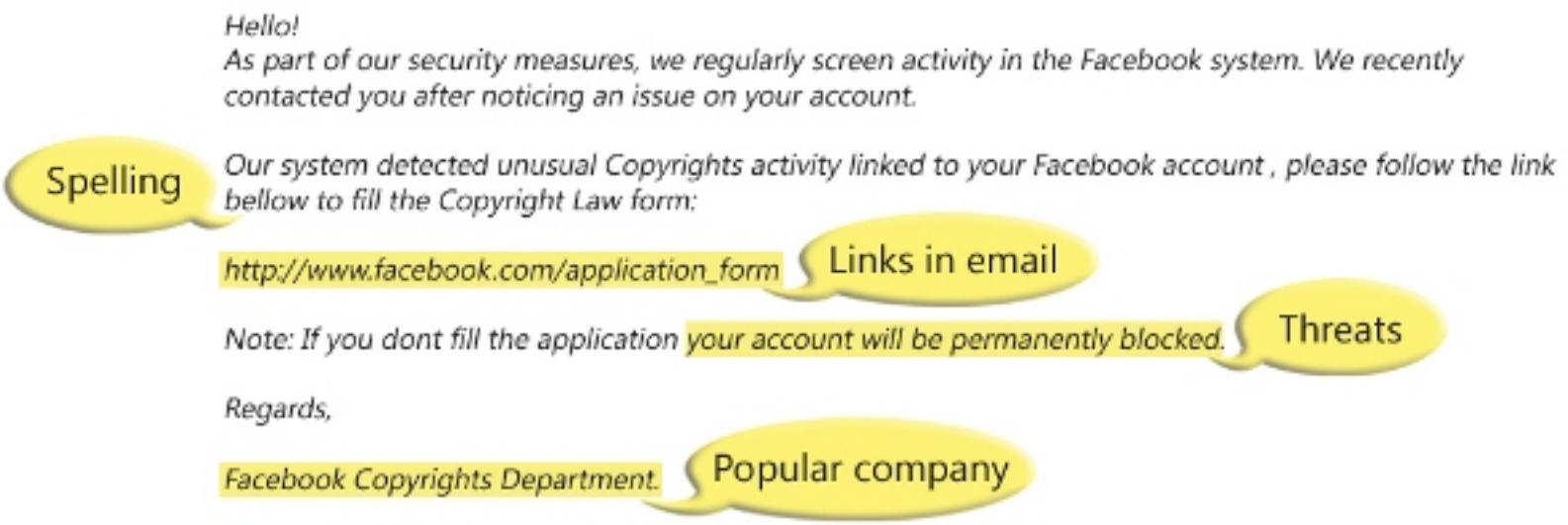
Phishing

- Definition?
  - "practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information"
    - Often involves spoofed email addresses
- Goal?
  - Preys on fear or greed to encourage people to voluntarily hand over personally identifiable information or account details

Phishing

- Examples:
  - Current Events/Charities
  - Tech Support
  - Financial
  - Government

Elements of a Phishing Message



http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

Spoofing E-mail

The Dubious “From” Field

- E-mail can appear to come from ANYONE ANYWHERE


NOT SURE IF PHISHING SCAM
OR IF IT DEPT MOVED TO NIGERIA...,
memegenerator.net

How to Spot a Phish

- "From" field **legitimate expected** address ?
- Greeting individualistic or generic?
- Spelling/grammar mistakes?
- Fear/greed language?

How to Spot a Phish

- URL hover?
- **Legitimate expected** signature?
- **Legitimate expected** attachment?
- Attachment explanation?

HINT: email does not come from official "@buffalo.edu" address

From: UB Technical Support <supportmessaging@abusemessage.buffalo.edu>
Date: May 23, 2013, 6:30:27 AM EDT
To: [redacted]@buffalo.edu
Subject: Urgent Message, Please Read

HINT: hovering on images/URLs shows you they do not link to "buffalo.edu"

ATTENTION UB,

Your email has been spammed too many times demanding for your email and password in other to protect your email account from been hacked further. The University board has decided to protect your account in a secured manner. This means helps in encrypting your password in our database to protect you from receiving spammed message.

ACTIVATE YOUR EMAIL PROTECTION LINK HERE

http://www.junewon.org/pm/images/Horde.htm

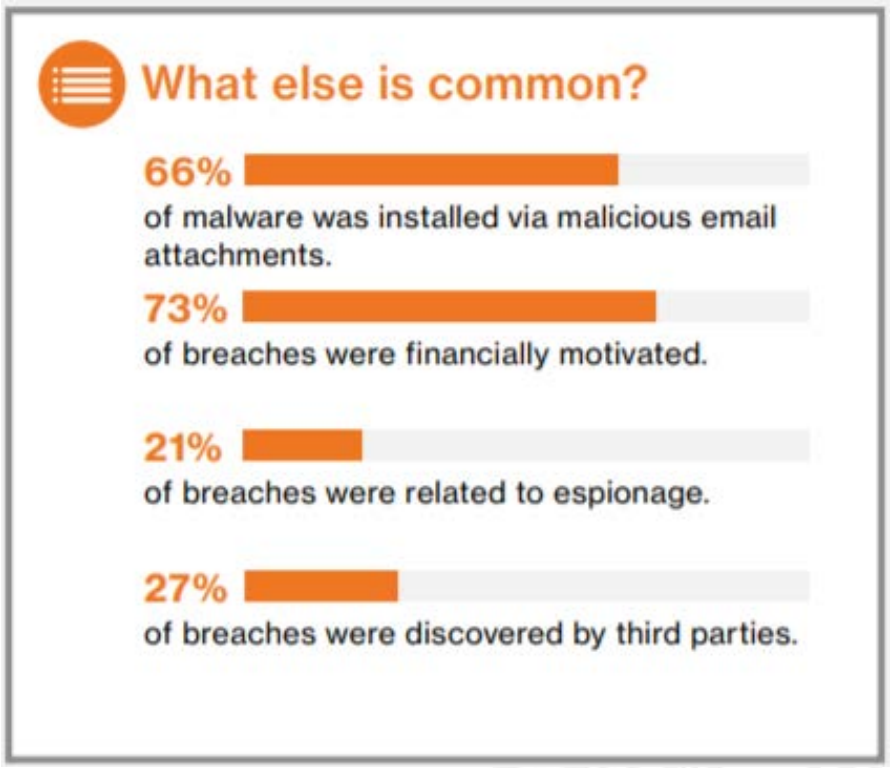
Admin Support

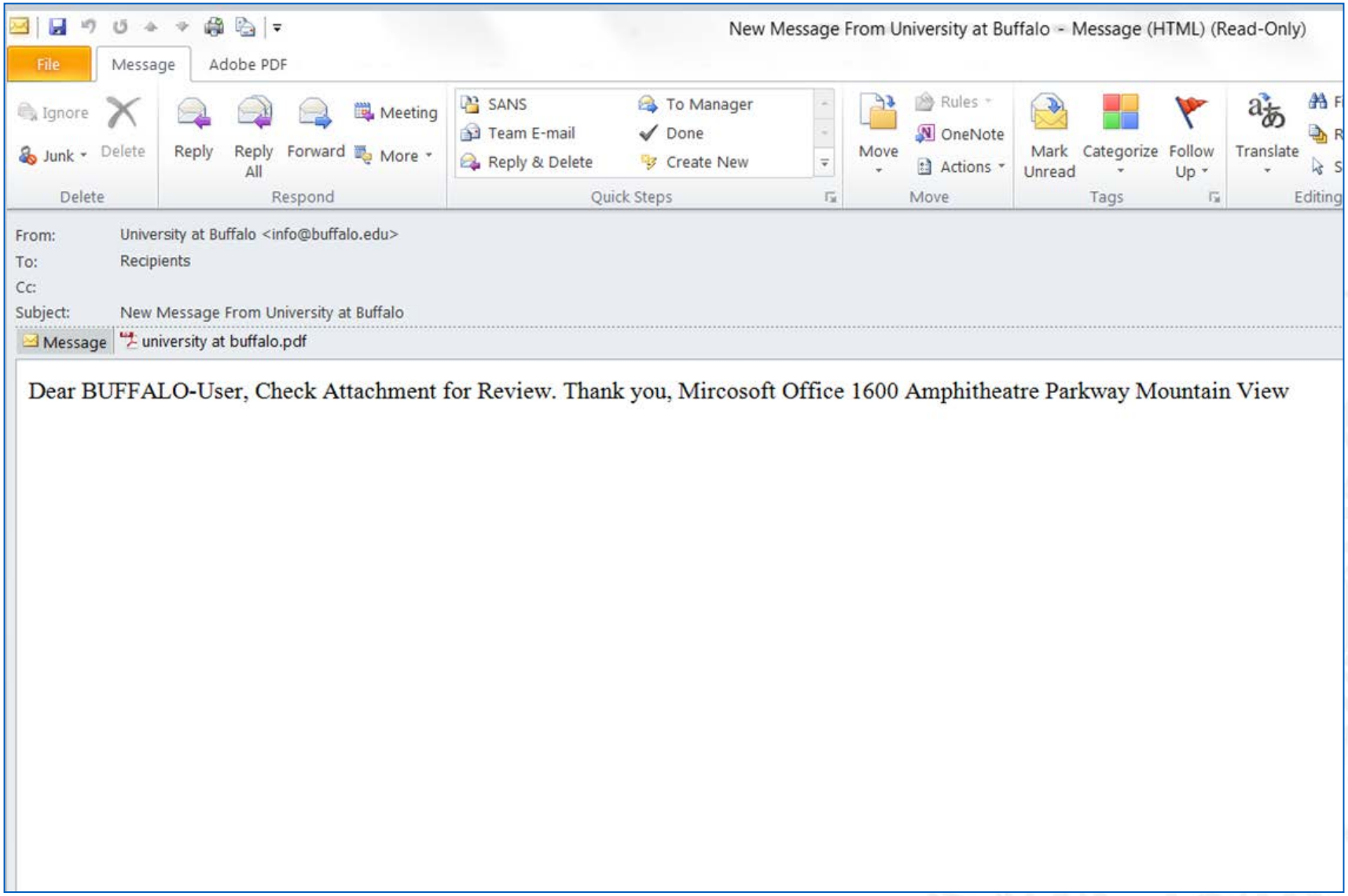
HINT: grammar


TRIES TO EMAIL, FORGETS ATTACHMENT,
SENDS TO THE WRONG PERSON
makeameme.org

Malware via Email Attachments

- According to the 2017 Verizon Data Breach Report, 66% of malware was installed via malicious email attachments




New Message From University at Buffalo - Message (HTML) (Read-Only)
File
Message
Adobe PDF
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
More
SANS
Team E-mail
Reply & Delete
To Manager
Done
Create New
Move
Rules
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Delete
Respond
Quick Steps
Move
Tags
Editing
From: University at Buffalo <info@buffalo.edu>
To: Recipients
Cc:
Subject: New Message From University at Buffalo
Message
university at buffalo.pdf
Dear BUFFALO-User, Check Attachment for Review. Thank you, Mircosoft Office 1600 Amphitheatre Parkway Mountain View

-------- Original Message --------
Subject: Annual Form - Authorization to Use Privately Owned Vehicle on State Business
Date: Tue, 8 Oct 2013 15:48:37 +0000
From: Lola Ferrell <Lola@buffalo.edu>
To: @buffalo.edu

All employees need to have on file this form STD 261 (attached). The original is retained by supervisor and copy goes to Accounting. Accounting need this form to approve mileage reimbursement.

The form can be used for multiple years, however it needs to re-signed annually by employee and supervisor.

Please confirm all employees that may travel using their private car on state business (including training) has a current STD 261 on file. Not having a current copy of this form on file in Accounting may delay a travel reimbursement claim.

Form_buffal...u.zip (10 KB)

Very Successful UB Phishing Example

Hi

Dear Dr. **[REDACTED]**:

I recently read your good article: "**[REDACTED]**" It's very useful in my field of research.
I wonder, if possible, to send me these articles to use in my current research:

1- http://websso.it.**[REDACTED]**.edut.in/login.php?url=http://www.sciencedirect.com/scien
<http://websso.it.**[REDACTED]**.edut.in/login.php?url=http://www.sciencedirect.com/scienc
edirect.com/science/article/pii/S03085961100HT00216>
ce/article/pii/S03085961100HT00216<http://websso.it.**[REDACTED]**.edut.in/login.php?url
=http://www.sciencedirect.com/sciencedirect.com/science/article/pii/S03085961100HT0021
6>

2- http://www.sciencedirect.com/science/article/pii/S0047272702001871

Thanks for you Cooperation in Advance.

Assoc. Prof. **[REDACTED]**

How serious??

- 87 accounts provided to ISO office as potentially compromised
- 67 actually compromised accounts
- Therefore, 77% of recipients were victims of this scam

Reporting Social Engineering

- How to report phishing at UB:
  - http://www.buffalo.edu/ubit/service-guides/safe-computing/report-phishing-attempt.html

Reporting Social Engineering

- How to report impersonation:
  - UBPD if on campus (645-2227)
  - Local PD if elsewhere
  - Social medial/account impersonation – directly to company

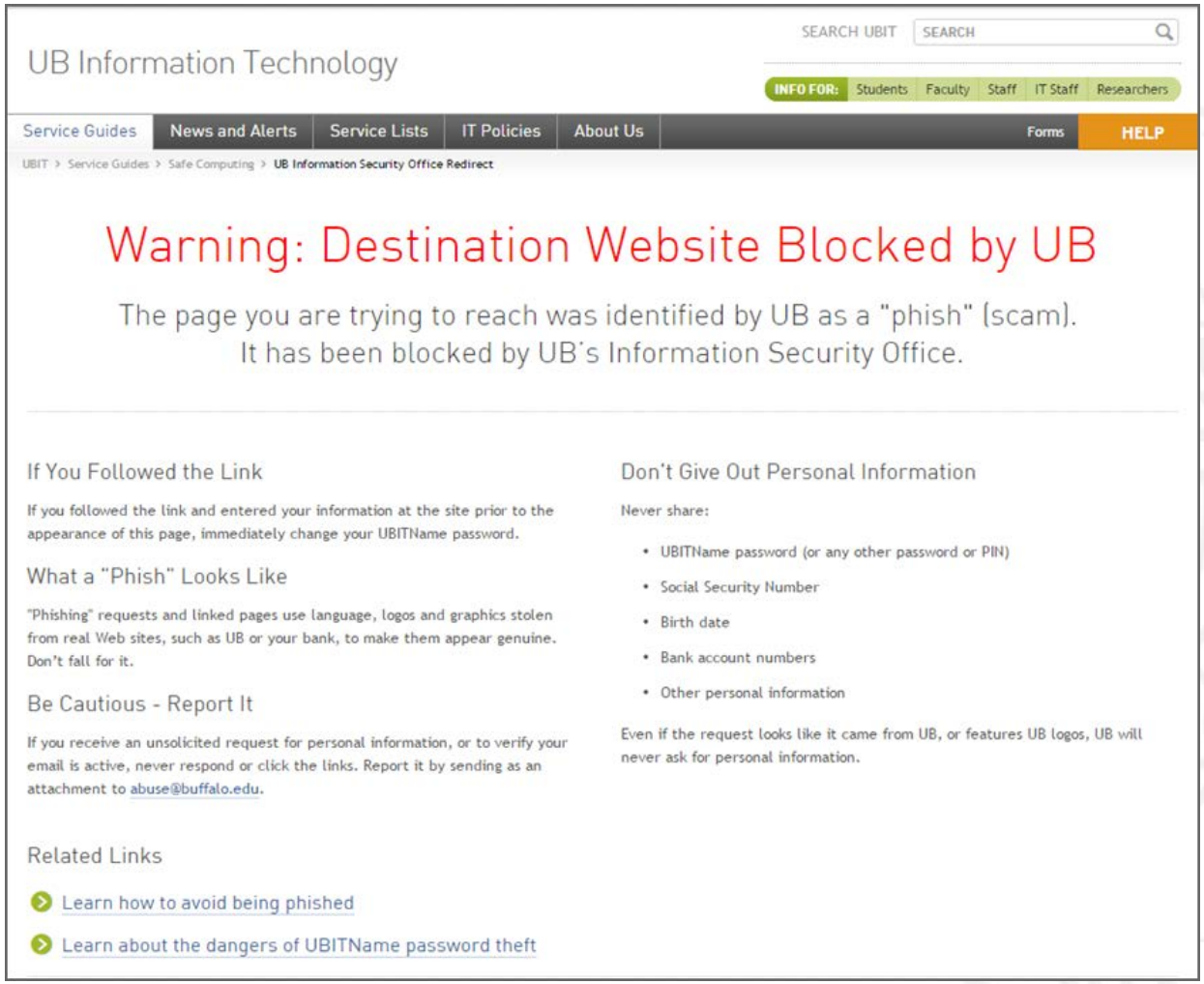
Reporting Social Engineering

- How to report vishing/smishing:
  - Report fraud to www.ftc.gov or call (888) 382-1222
    - Need number and name from caller ID, time of day, any info discussed/heard
  - Victims can also contact the Internet Crime Complaint Center: https://www.ic3.gov/complaint/default.aspx
  - Unwanted commercial mobile phone calls/e-mail messages: 1-888-CALL-FCC.

Unsubscribe?

- Only if you/department actually subscribed!

Education through Redirection



UB Information Technology

SEARCH UBIT SEARCH

INFO FOR: Students Faculty Staff IT Staff Researchers

Service Guides | News and Alerts | Service Lists | IT Policies | About Us | Forms | HELP

UBIT > Service Guides > Safe Computing > UB Information Security Office Redirect

Warning: Destination Website Blocked by UB

The page you are trying to reach was identified by UB as a "phish" (scam).
It has been blocked by UB's Information Security Office.

If You Followed the Link

If you followed the link and entered your information at the site prior to the appearance of this page, immediately change your UBITName password.

What a "Phish" Looks Like

"Phishing" requests and linked pages use language, logos and graphics stolen from real Web sites, such as UB or your bank, to make them appear genuine. Don't fall for it.

Be Cautious - Report It

If you receive an unsolicited request for personal information, or to verify your email is active, never respond or click the links. Report it by sending as an attachment to abuse@buffalo.edu.

Related Links

- Learn how to avoid being phished
- Learn about the dangers of UBITName password theft

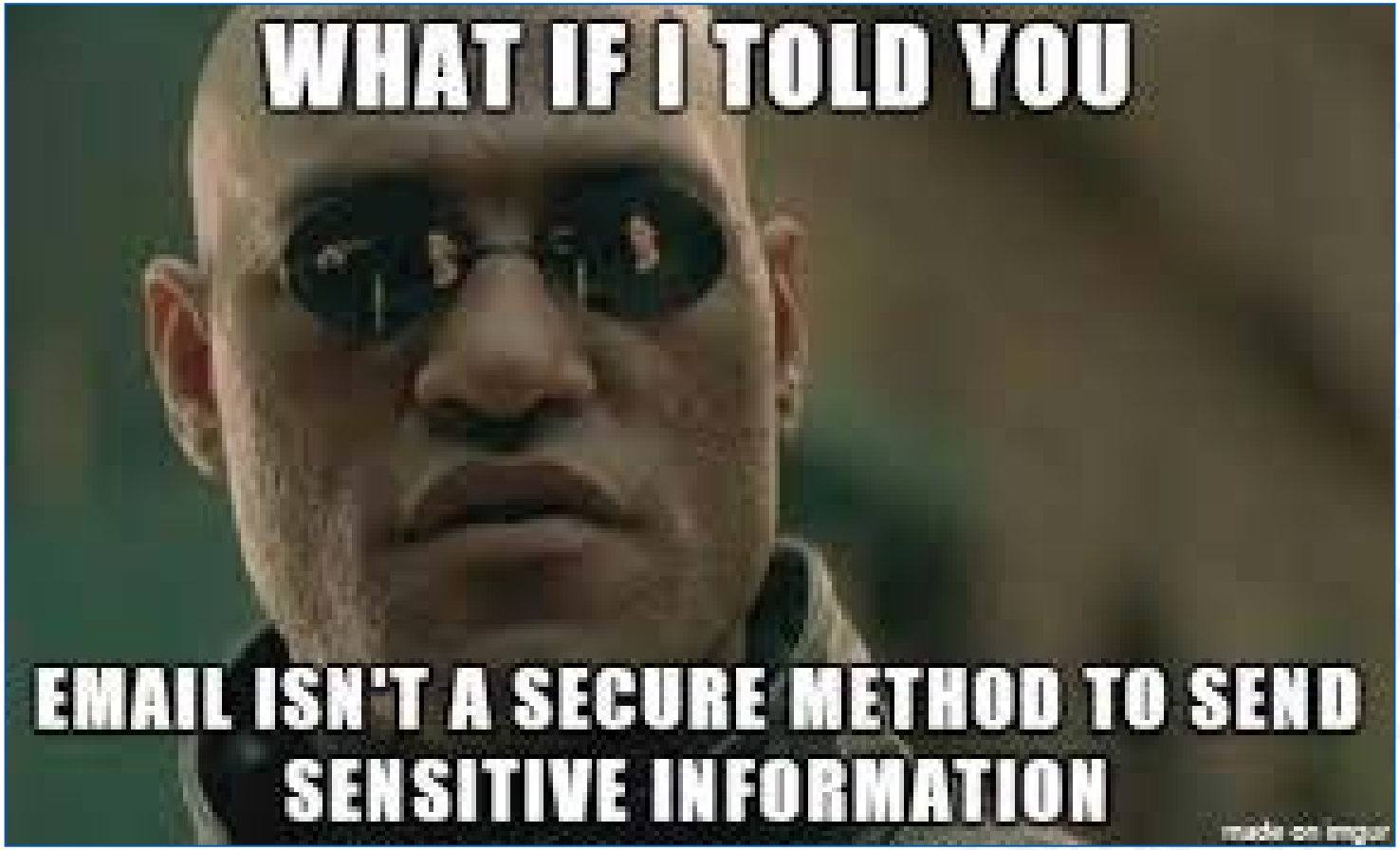
Don't Give Out Personal Information

Never share:

- UBITName password (or any other password or PIN)
- Social Security Number
- Birth date
- Bank account numbers
- Other personal information

Even if the request looks like it came from UB, or features UB logos, UB will never ask for personal information.

Secure Communications?



Questions?

With Gratitude

- To YOU for listening and the organizers of UB Business Day for allowing me to share these thoughts with you

- To the folks who originally created the images, videos, and other creative content – thank you!

(Note that this content was used in accordance with copyright law – if you want to quote, please give credit where it is due!)