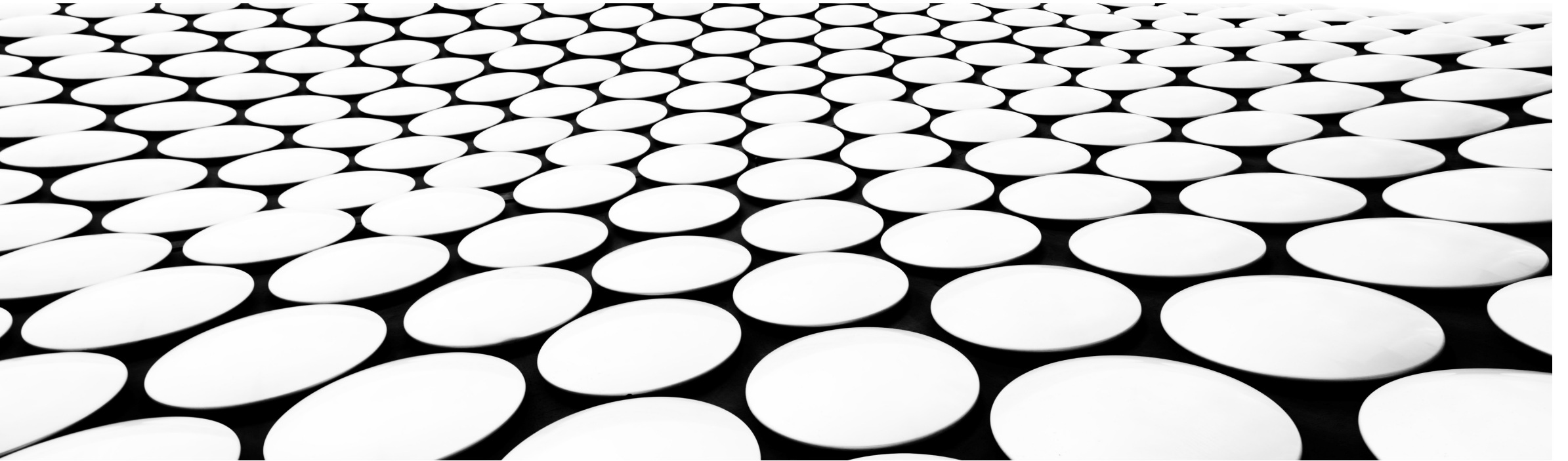# SOCIAL ENGINEERING & PHISHING

CAN YOU TELL WHO IS WHO?

SOCIAL ENGINEERING: THE ART OF HUMAN MANIPULATION

Social engineering is the exploitation of human psychology, rather than technical hacking techniques to gain information or access to that information.

The "ishings"	Other types
Phishing	Honey Trap
Spear Phishing	Watering Hole
Whaling	Scareware
Vishing	Pretext (pretending to be someone else)
Smishing	Diversion Theft
	Piggyback or Tailgate

THE MANY TYPES OF SOCIAL ENGINEERING

HOW EASY IS IT FOR A SOCIAL ENGINEER TO GET YOUR INFORMATION?

- You may not be the one giving away your information.

- Video time!

- This is how hackers hack you using simple social engineering

Scam Call Victims & Money Lost Over a 5-Year Period in the US

Legend:
- Total Americans that lost money to scam calls (blue)
- Total money lost to scam calls (red)

Year	Total Americans that lost money	Total money lost
2015	27.1 million	$7.4 billion
2017	22.1 million	$9.5 billion
2018	24.9 million	$8.9 billion
2019	43 million	$10.5 billion
2020	56 million	$19.7 billion

99FIRMS.COM

Source: Truecaller

HOW TO PREVENT SOCIAL ENGINEERING ATTACKS

Determine — Determine whether an email has been spoofed by hovering over the sender's name to make sure it matches the email address and checking the email address for spelling errors and other common giveaways.

Be Suspicious — Be suspicious of any unsolicited communication, especially from someone they don't know.

Avoid — Avoid downloading suspicious email attachments.

Hover over — Hover over links in emails to make sure the website URL is valid.

Verify — Verify someone's identity through an alternate contact method (e.g., in person or by calling them directly) before providing any sensitive information.

HOW ORGANIZATIONS ARE INFILTRATED BY VISHING (AND OTHER ATTACKS)

Call centers, such as our service desk, are high targets for people impersonating others.

- Urgent request with a deadline

- Desperately in need of assistance

- Threatening tone

Another example of vishing, in a business setting:
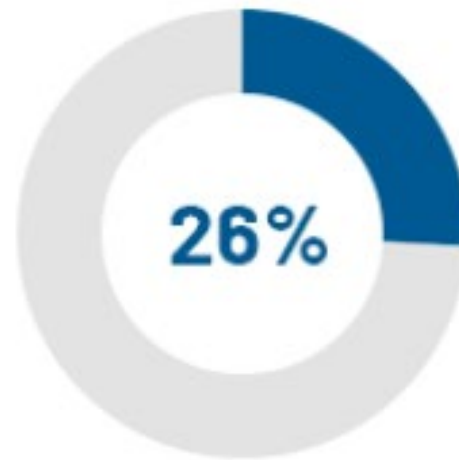
Watch this hacker break into a company

Common Email Spam File Types

94% of malware is delivered via email

45% Office doc files

26% Windows apps

22% Other

99FIRMS.COM

Source: Verizon

Phishing @ UTHSC

Do	Don't
Keep your software and browsers up to date	Click on any links in any email sent from unknown or suspicious senders
Hover over links to identify obvious fakes; make sure that an embedded link is taking you to the exact website it purports to be	Send an email the looks suspicious to friends or family as this could spread a phishing attack to unsuspecting loved ones
Take your time and inspect emails for obvious red flags: misspelled words and bad grammar, incorrect URL domains, unprofessional and suspicious visuals and unrecognized senders	Download content that your browser or security software alerts you may be malicious
Instead of clicking on a link provided in an email, visit the website of the company that allegedly sent the email to make sure the deal being advertised is also on their webpage	Give away personal information like your credit card number, home address, or social security number to a site or email address you think may be suspicious

LET'S SEE WHAT WE HAVE HAD TO DEAL WITH!

ACTUAL PHISHING EMAILS REPORTED TO ABUSE@UTHSC.EDU

Dear **Diana Yeung**,

Welcome to the UTHSC online application! We hope that you will find this application easy to use and understand.

Your **UTHSC** ID is: 8580598359. Please include your UTHSC ID Number in all communications with UTHSC customer support and your designated programs.

Once your application is submitted it will be in a "Received" status and the review process will begin. Before your application can be verified, however, your application must have a status of "Complete" and be assigned a Complete Date. For your application to become Complete, the following steps must occur:

1. Application is e-submitted.
2. All required transcripts and/or any required foreign transcript evaluation(s) have been received at:
   UTHSC
   P.O. Box 9141
   Watertown, MA 02471
3. All required test scores have been officially reported and received by the Graduate Programs Office.

From: Wendy Likes <likeswendy6@gmail.com>

Date: Saturday, August 7, 2021 at 8:47 AM

To: Wills, Christina <cwalla30@uthsc.edu>

Subject: [Ext] Send me your available cell number

--

Wendy Likes, PhD, DNSc, APRN-Bc, FAANP

Dean of College of Nursing

College of Medicine, Department Obstetrics & Gynecology

From: John Lithgow <samosarmok149@gmail.com>

Date: Tuesday, September 14, 2021 at 3:39 PM

To: Guyot, Shannon <sguyot@uthsc.edu>

Subject: [Ext] Invoice _Id: EYB-4668737_88

NORTON

Dearsguyot@uthsc.edu,

We have received your order successfully.

In addition to selecting Norton services, we have activated them and deducted the amount appropriate.

I_nvoice Id

Invoice _Id: EYB-4668737

Charges: USD 188.65

Payment mode: Auto Pay

Date: Sept 14, 2021

Requesting a refund or having an issue with this transaction,

Contact at us **+1 (805) 419-9664**

From: kjones62 <info086896@emailsrvrcom.com>
Sent: Monday, July 26, 2021 9:25 AM
To: JONES, KIMBERLEY M <kjones62@uthsc.edu>
Subject: [Ext] W.H.O World Lottery Program on COVID-19

This is to inform you that your email address was automatically selected in the current COVID-19 Pandemic relief programme currently organzied by the World Health Organization worldwide.

Kindly provide necessary informations as attached to the email to file your claim.

Thanks

Mr. Kwabena Agyei
Lottery Cordinator.
Covid-19 Pandemic Debt Relief Program.
World Health Organization.
E-mail:info@thewealthinvest.com

From: Bingham, Ciara Cassandra <cbingha5@vols.utk.edu>
Date: Friday, September 10, 2021 at 9:31 AM
To:
Subject: NOTICE FROM MICROSOFT

Our record indicates that you recently made a request to terminate your Office 365 email. And this process has begun by our administrator.

If this request wa https://forms.gle/5at6chfupptzcogy8 ive no knowledge of it, you are advised to verify your Account
Click or tap to follow link.

CLICK HERE TO VERIFY

From: ████████████████████████████

Sent: Thursday, August 16, 2018 2:10 PM

To: ████████████████████████████

Subject: Re: BIWEEKLY TIME SHEETS

Unable to display this message

Click here to view message

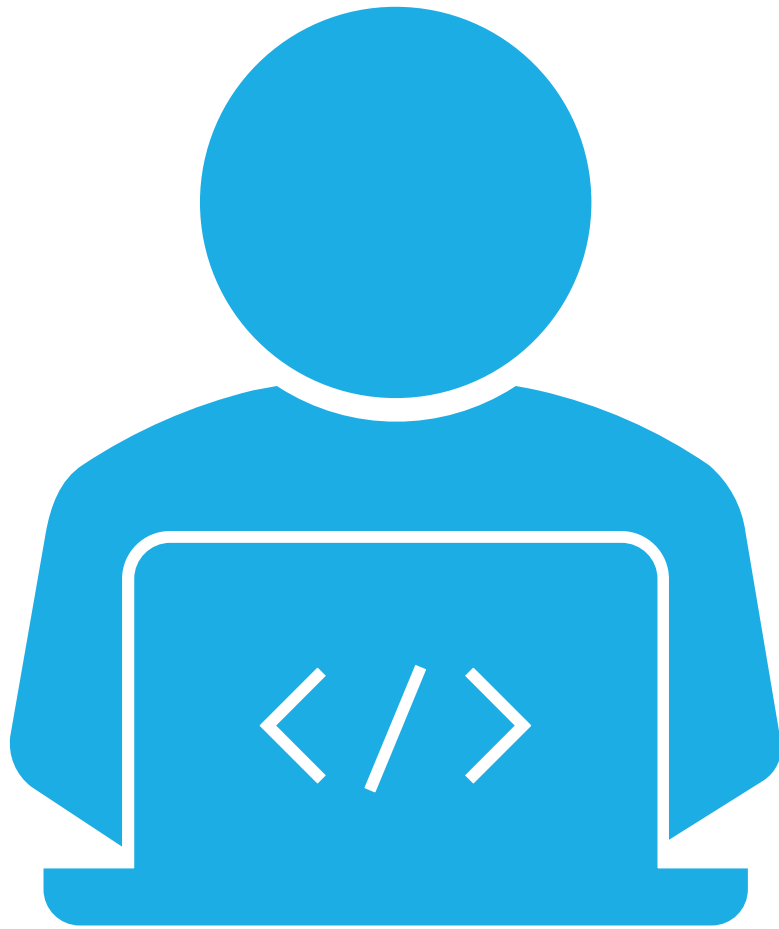Imap message delayed: 1Qmg - Date: 08/16/2018 7:09:50 (uthsc)

Can't end on such a serious note!

If what you received via email was done in person, there would be no way you would fall for it.

The Defence Works Sketches   Phishing Emails in Real Life   Funny Security Awareness Training

CONTACT INFORMATION

Chris Madeksho – Cybersecurity Analyst

mmadeksh@uthsc.edu

901.448.1579

Office of Cybersecurity

itsecurity@uthsc.edu

901.448.1860

https://uthsc.edu/its/cybersecurity/

QUESTIONS?