



THOMAS MORE
UNIVERSITY

Phishing Training



WHAT IS PHISHING?



- Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.
- Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than trying to break through a computer's defenses.

<https://searchsecurity.techtarget.com/definition/phishing>



WHAT TO LOOK FOR



“Quick Tips”

- Spelling errors, lack of punctuation or poor grammar
- Hyperlinked URL is different from the one displayed
- Threatening language that calls for immediate action
- Requests for personal information
- Announcement indicating you won a prize or lottery
- Requests for donations



EXAMPLE OF A FAKE EMAIL



Inbox (helpdesk) Filter

Next: No more events for today or tomorr...

IT Helpdesk
Urgent Alert 11:39 AM
Hello, We have noticed some suspicious ...

Last week

Adobe Cr...
Free online co...
Expand your digital skills and explore best ...

Abrams, Sierra Kath...
MY EMAIL Thu 4/12
Hello, I have been having a problem with...

Adobe Systems
Adobe Spark for the classroom Thu 4/12
Free creative apps with enhanced data pr...

Garnick, Erin
RE: Technology Training - Wee Wed 4/11
I will attend friday From: Kelley, Shelly Sen...

Kelley, Shelly
Technology Training - Week o Wed 4/11
To: Faculty and Staff IT Services will be pr...

iCloud
Your iCloud storage is almost Tue 4/10
Dear Thomas More IT, Your iCloud storage...

Urgent Alert

IH IT Helpdesk <thomasmoreit55@gmail.com>
Today, 11:39 AM
helpdesk

Illegitimate Email

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, [click here](#).

To always show content from this sender, [click here](#).

Hello,

We have noticed some suspicious on your account. We have locked your account until we are able to verify this is you. Please click on the link and enter your password so we can reactivate your account.

<http://password.thomasmore.edu> **Links in email**

Your account will be DEACTIVATED if you do not verify your account. **Threats**

Thanks,

IT Center

Claims to come from IT Helpdesk

Reply all

EXAMPLES AT THOMAS MORE



From: John Smith <sarahwitt2013@gmail.com>

Sent: Monday, October 1, 2018 4:17:11 PM

To: Thomas Jefferson

Subject: Hello

Good Day,

Are you in the office ? I have an assignment i need you to do for me.I am in a meeting i won't be able to pick a call.

Thanks

- Claims to come from John Smith
 - Actual email address says (sarahwitt2013@gmail.com)
 - Calls for immediate action: “I have an assignment I need you to do for me.”
 - Incorrect grammar: “i” is not capitalized. Also forgot spaces.



EXAMPLES AT THOMAS MORE



From: John Smith <sarahwitt2013@gmail.com>

Sent: Monday, October 1, 2018 4:27:44 PM

To: Thomas Jefferson

Subject: Hello

I need Itunes Gift cards of 100\$... 6 piece, that's 600\$ worth of Itunes Cards...scratch the code panel and take a clear picture of it and send to me here in the email, Ensure you keep the cards until i ask you to dispose off,Sorry for the inconvenience,Will reimburse that back to you.

Thanks.

Note..I need it asap

- Asks for an item worth value
 - Wanted iTunes Gift Cards sent to them: \$600 worth
 - Calls for immediate action again: “Note..I need it asap”



IT IS YOUR RESPONSIBILITY



- YOU and only YOU can protect your account
- Be the “Grammar Police” and keep an open eye out
- “Don’t get hooked” or be a victim of a phishing email
- Make sure you know what you are clicking on
- Think before you click
 - Am I expecting this email
 - Do I know the sender
 - Are there any suspicious links



WHAT THEY MAY SAY



These phrases are common when you receive a phishing email

- Official Data Breach Notification (14%)
- UPS Label Delivery IZBE3I2TNY000I50I1 (12%)
- IT Reminder:Your Password Expires in Less Than 24 Hours (12%)
- Change of Password Required Immediately (10%)
- Please Read Important from Human Resources (10%)
- All Employees: Update your Healthcare Info (10%)
- Revised Vacation & Sick Time Policy (8%)
- Quick company survey (8%)
- A Delivery Attempt was made (8%)
- Email Account Updates (8%)

<https://www.netsec.news/effective-phishing-emails-revealed/>



HOW TO PROTECT YOURSELF



Refuse the Bait!

- If you do not know the person then use your “Quick Tips”
- Think before you click
- Verify the website
- Never give out personal information
- Do not click on pop-ups or links
- Ask yourself:
 - Am I expecting this message?
 - Is this message from someone I know?
 - Does the email address match the name of the sender?
 - Does the message sound like it’s coming from the sender?



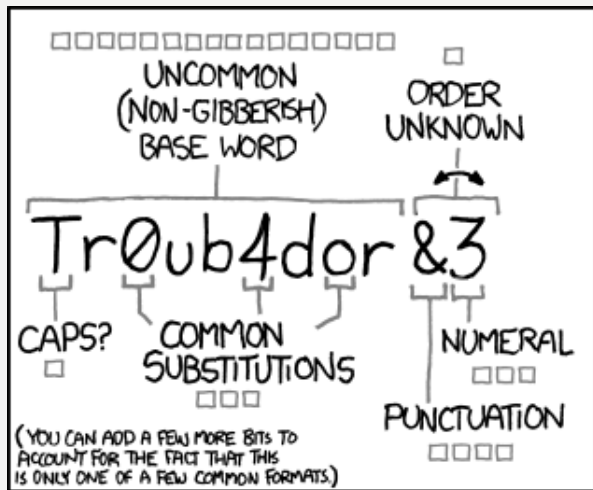
PASSWORDS




- You should not use the same password for multiple accounts/websites.
- You should not tell anyone your password
- Do not write down your password and keep it by your computer
- Your passwords should be
 - Easy to remember but hard to guess
 - Long and hard to decrypt
 - Changed on a regular basis
 - Have multiple characters including special characters
- Use a password manager to keep passwords secure
 - KeePass
 - 1Password

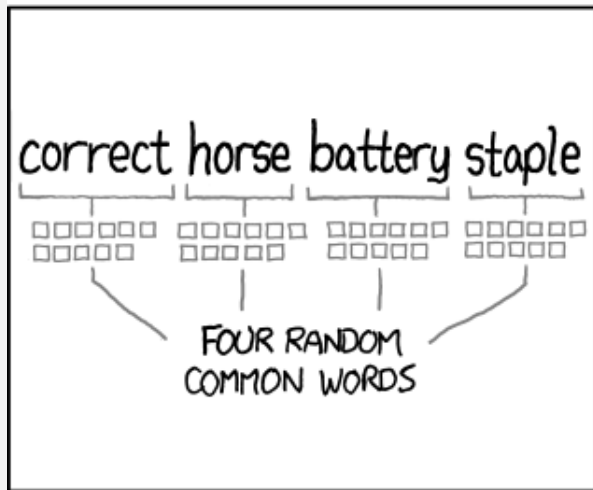


XKCD COMIC

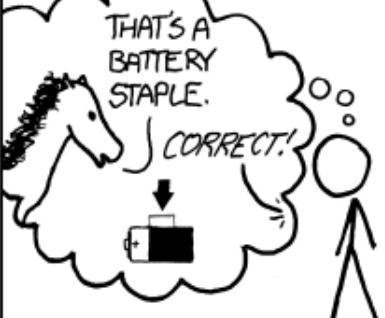


~ 28 BITS OF ENTROPY
□□□□□□□□ □
□□□□□□□□ □
□□□□ □□□□
 $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOKEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?
AND THERE WAS SOME SYMBOL... 
DIFFICULTY TO REMEMBER: **HARD**



~ 44 BITS OF ENTROPY
□□□□□□□□□□ □□□□□□□□□□
□□□□□□□□□□ □□□□□□□□□□
□□□□□□□□□□ □□□□□□□□□□
 $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.  CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



WHAT TO DO IF YOU THINK YOU ARE A VICTIM OF PHISHING



Don't panic! We can help! Contact the IT Help Desk!

Contact IT Services by:

- Browsing to helpdesk.thomasmore.edu
 - calling **859-344-3646**
 - emailing helpdesk@thomasmore.edu
 - or stopping by the helpdesk inside the computer center (lower level of main administration building)

