

How to Recognize and Defend Against Phishing

Presented by:

Todd Janiak, Technology Services &
Support Manager

Jack Crawford, Cyber Club President



10/18/2023



Todd Janiak

- Technology Services & Support Manager for Baker College
- Baker Employee - 10 years
- Bachelors of Science - Information Technology and Security
- Master of Science - Information Systems



Jack Crawford

- Baker Cyber Club President,
Cyber Defense Team Member
- Student pursuing Bachelors of Science -
Information Technology and Security
- +3 Years of experience in Tech Support and
Loss Prevention



What is Phishing?

According to the Cybersecurity & Infrastructure Security Agency, Phishing occurs when a criminal attempts to trick users into opening harmful links, emails, or attachments in the hopes of obtaining personal information.

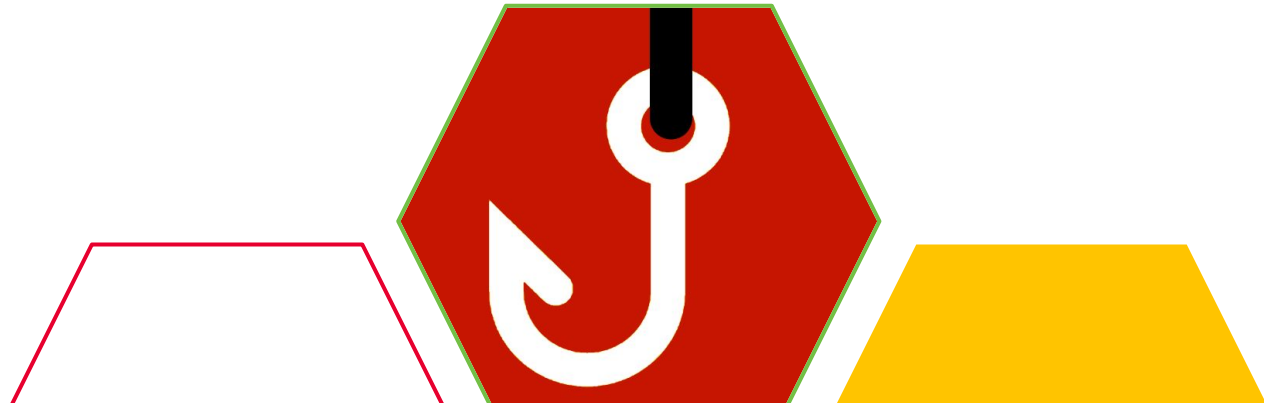
Like with real fishing, cyber phishers attempt to get you to take their bait for their own personal gain.



What is the goal of Phishing?

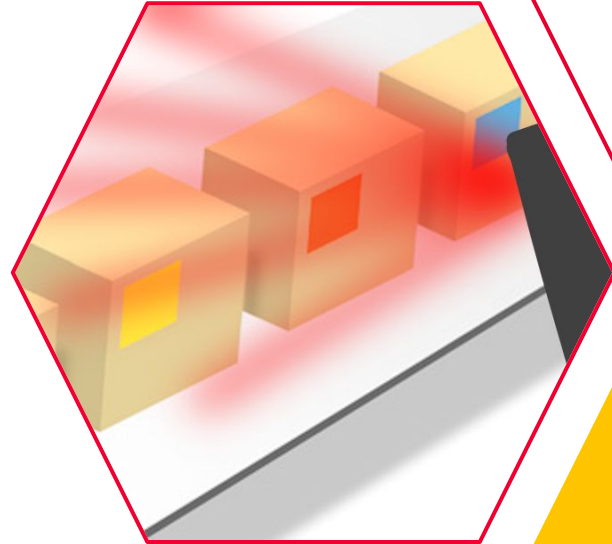
Phishing is a form of social engineering. Attackers bypass security by convincing trusted users to grant them access or give them information.

Phishing attacks are adaptive and dangerous when taken lightly. They can be used in isolation to elicit funds, or as part of a greater attack. The scammer shapes their phishing attack around their target audience and attack's goal.



The Stats on Phishing:

- There were more than 4.7 million attacks in 2022, with 1.35 million in the fourth quarter alone.
 - This represents consistent growth of 150 percent per year since 2019.
- In recent years, phishing has shifted away from wider scams into more targeted attacks. Last year, over 75% of phishing was targeted.
- Verizon has consistently reported phishing as one of the top threat action varieties.
 - Last year Verizon reported 30% of data breaches incorporated phishing.
- SSL is not as safe as it once was. 84% of phishing sites examined in an APWG report use SSL, despite many directing users to check for HTTPS:// in the URL.
 - This percentage grows by 3% every quarter!



Types of Phishing Attacks

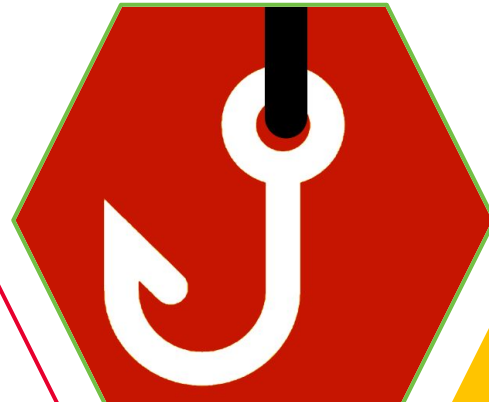


Deceptive Phishing

Deceptive phishing is the most common attack and the base of all others.

All phishing relies on deception to retrieve the desired information. Reports tell us that **96%** of phishing attempts are made to gather intelligence.

“Deceptive Phishing” refers to phishing techniques that are not specialized or tooled to target a specific victim or audience.

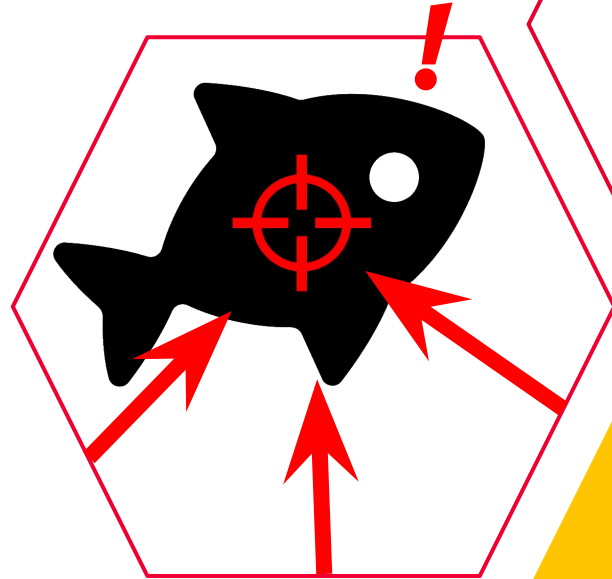


Spear Phishing

Spear Phishing - A phishing scheme targeting a specific target.

Spear phishers often use data they have on the target to make more convincing lures.

Public-facing information is easily gathered from social media.



Whaling

Whaling - A subset of spear phishing, Whaling attacks that target senior staff.

Whaling schemes imitate internal communications.

Attacks exploit internal power structures, faking instructions from your superiors or peers.



Smishing / Vishing

Smishing - Phishing through SMS spoofing or solicitation.

Smishing attacks most commonly imitate SMS alerts from a bank or other financial institution.

Vishing - Phishing through voice calls or caller campaigns.

Voice AI has spawned a new wave of vishing, including faked kidnappings.



**Irwin, 2023 / Karimi, 2023*

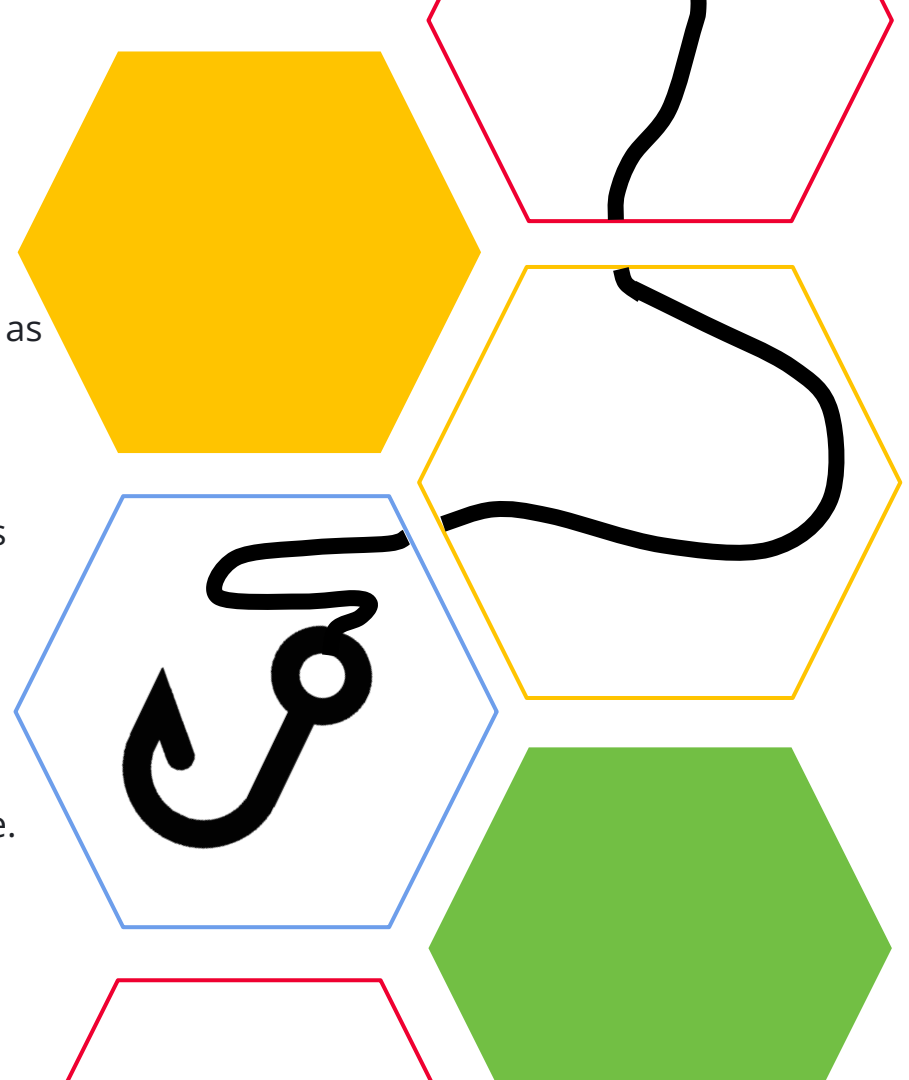


Angler Phishing

Angler Phishing - Phishing users while doubling as users or official accounts on Social Media

Victims seemingly initiate contact with scammers with this method.

Frequent changes to social media accounts and sites keeps the attack fresh and difficult to notice.



Recognizing a Phishing Attack



Example #1

- From address is not from Cracker Barrel
- Recipient is just an email address
- A sense of urgency
- Brief with few details

From: Cracker Barrel <gift@crackerbarrel.food-mailer.com>
Reply-To: Cracker Barrel <gift@crackerbarrel.food-mailer.com>
Subject: Claim your Cracker Barrel Gift card!

Template ID: 215754-5578949

 Send Me a Test Email

Show Remote Images

 Toggle Red Flags



Hi j...@baker.edu,

Still haven't received your Cracker Barrel reward card?

We're sending this reminder because **your card is still pending**, and a few questions still need to be completed.

If the claim process isn't completed soon, your card may expire.

[Complete Registration](#)

Example #2

- The account is a major business operating an unverified account.
- The account is bypassing customer service channels.
- The response is sent via Radian6, a service for automating tweets, not a typical user.



The screenshot shows a Twitter profile for Domino's Pizza (@dominos) with a verified badge circled in red. The profile information includes the location "Ann Arbor, MI", the website "dominos.com", and the date "Joined April 2009". Below the profile is a tweet from a user with a redacted name, stating: "Finally here, cold as ice. Might as well have not brought it at all. Never ordering from @dominos again." The tweet is 22 hours old. A reply from Domino's Pizza (@dominos) follows, with the text: "@sreese25 Sounds like we dropped the ball and I'd like to help make this right! Can you pls follow/DM store info, your name, phone & email?". Below the reply are options for "Hide conversation", "Reply", "Retweet", "Favorite", and "Buffer". The tweet is timestamped "4:38 PM - 28 Apr 12 via Radian6 · Details".

Example #3

- Example of whaling and the imposter technique
- Sending domain appears legitimate
- No sender name
- Event details are missing
- No company branding

From: Baker College Holiday Team <holidays@baker.edu>
Reply-To: Baker College Holiday Team <holidays@baker.edu>
Subject: Halloween Potluck Signup

Template ID: 215754-5877440

 Send Me a Test Email

Show Remote Images

 Toggle Red Flags

Hi all,

You may have heard we've been planning our company Halloween potluck. Please review the [sign-up sheet](#) and see what people have signed up to bring. Let us know as soon as possible what you are bringing in so we can prepare.



Thanks so much for participating!

Baker College Holiday Team

Example #3


- Example of whaling and the imposter technique
- Sending domain appears legitimate
- No sender name
- Event details are missing
- No company branding

From: Baker College Holiday Team <holidays@baker.edu> **Template ID:** 215754-5877440
Reply-To: Baker C
Subject: Hallowee

Show Remote

Hi all,

You may have h
see what peopl
prepare.



Thanks so muc

Baker College Holiday Team

Template ID: 215754-5877440

Me a Test Email

Sign in - Google Accounts

Sign in

Use your Google Account

Email or phone

[Forgot email?](#)

Not your computer? Use Private Browsing windows to sign in. [Learn more](#)

[Create account](#) [Next](#)

English (United States) Help Privacy Terms

Self Assessment

From: Google <noreply@access-google.com>
Reply-To: Google <noreply@access-google.com>
Subject: Security Alert

Template ID: 215754-5877527

Show Remote Images

 [Send Me a Test Email](#)

 [Toggle Red Flags](#)



iOS was granted access to your Google Account

jv !@baker.edu

If you did not grant access, you should check this activity and secure your account.

[Check activity](#)

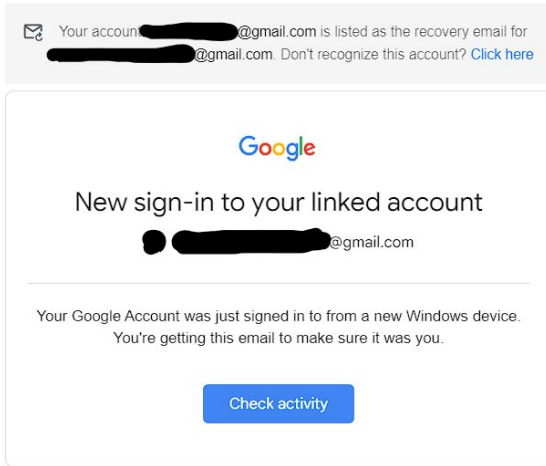
You can also see security activity at
<https://www.access-google.com/notifications/security-activity>

Self Assessment

Recovery Account:

Google <no-reply@accounts.google.com>
to me ▾

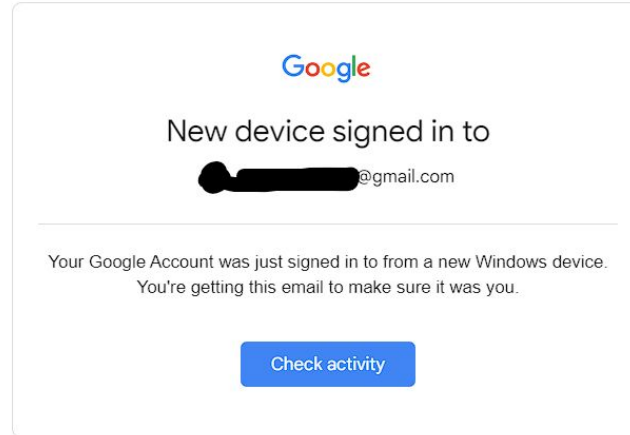
May 3, 2020, 5:37 PM ☆ ↶



You received this email to let you know about important changes to your Google Account and services.
© 2020 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Affected Account:

Google <no-reply@accounts.google.co...> Wed, Sep 30, 2020, 8:28 PM ☆ ↶ ⋮
to me ▾



You received this email to let you know about important changes to your Google Account and services.
© 2020 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

If you suspect phishing, compare the message to previous messages, or login to the account from a different browser or machine to check its status.

Redflags for Phishing :

- ❑ Am I being guilted, rushed, or pressured?
- ❑ Am I being contacted through a different address or method than usual?
- ❑ Am I being treated unprofessionally?
- ❑ Am I being asked to deliver confidential information?

Prevent being a Phishing Victim



Mail and Browse Mindfully

Like any hoax, phishing is best countered with healthy skepticism.

Phishers work like magicians, using graphics or enticing messages are used to distract the victim from realizing they are being phished.

Their scheme bets on victims coming across their message and missing details.

Tips for Mindful Browsing:

- Avoid answering or reading emails late at night or too early in the morning.
- Address burnout early, keeping your work attentive when online.
- Don't rely on multitasking to complete emails and other projects.
- Be skeptical of outrageous or inexplicable discounts or offers.

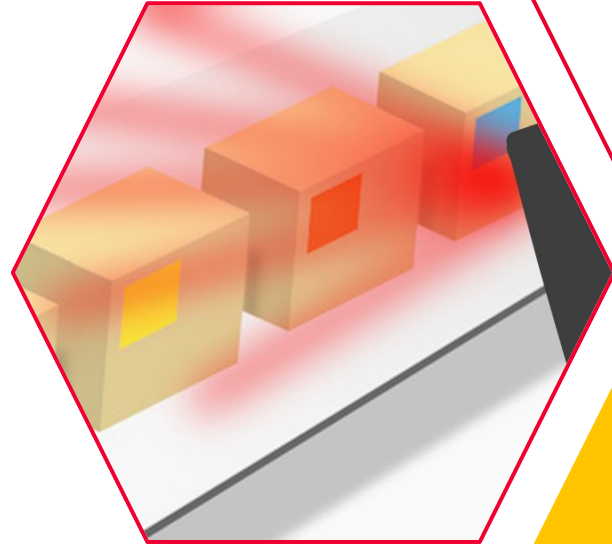
Flag and Filter Traffic

The first line of defense against phishing is flagging and filtering phishing emails and sites.

If you disable or manage security features, make sure to take notes and return to rennable them.

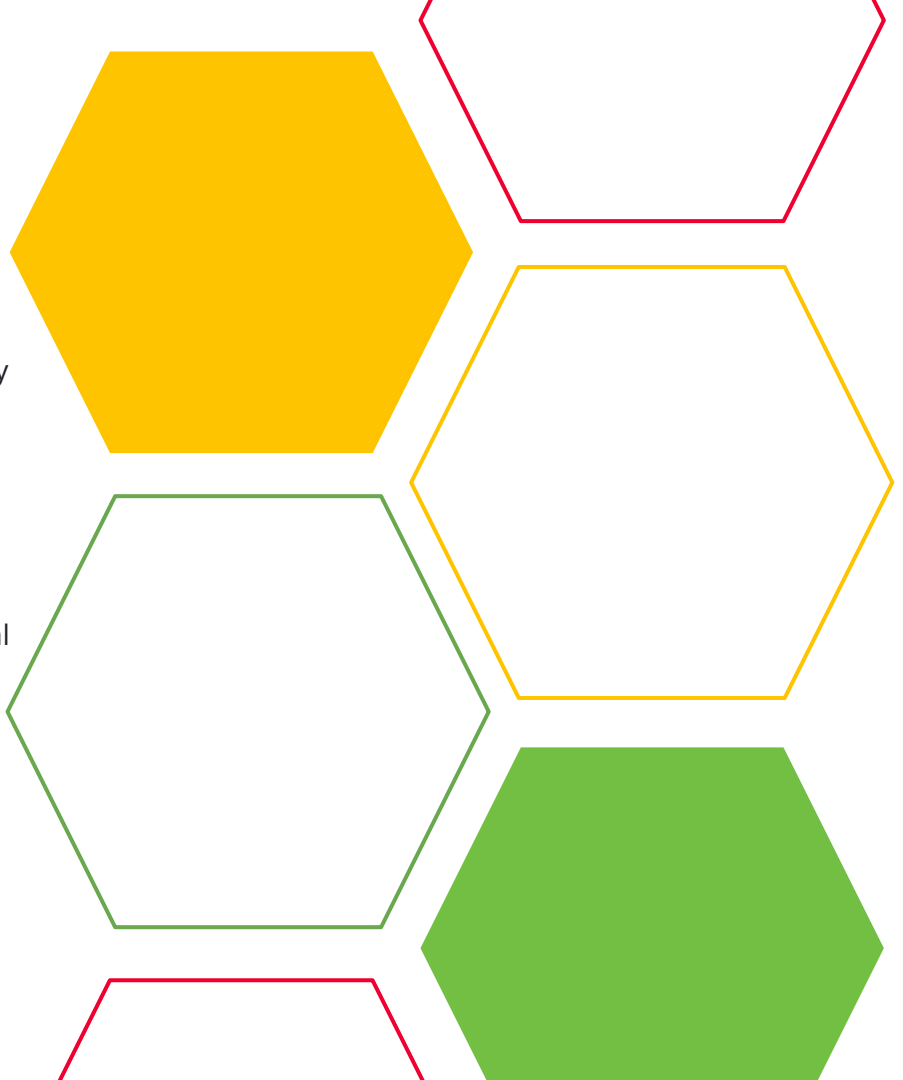
If you receive a phishing email, flagging it with your email client helps prevent it from returning, or harming others.

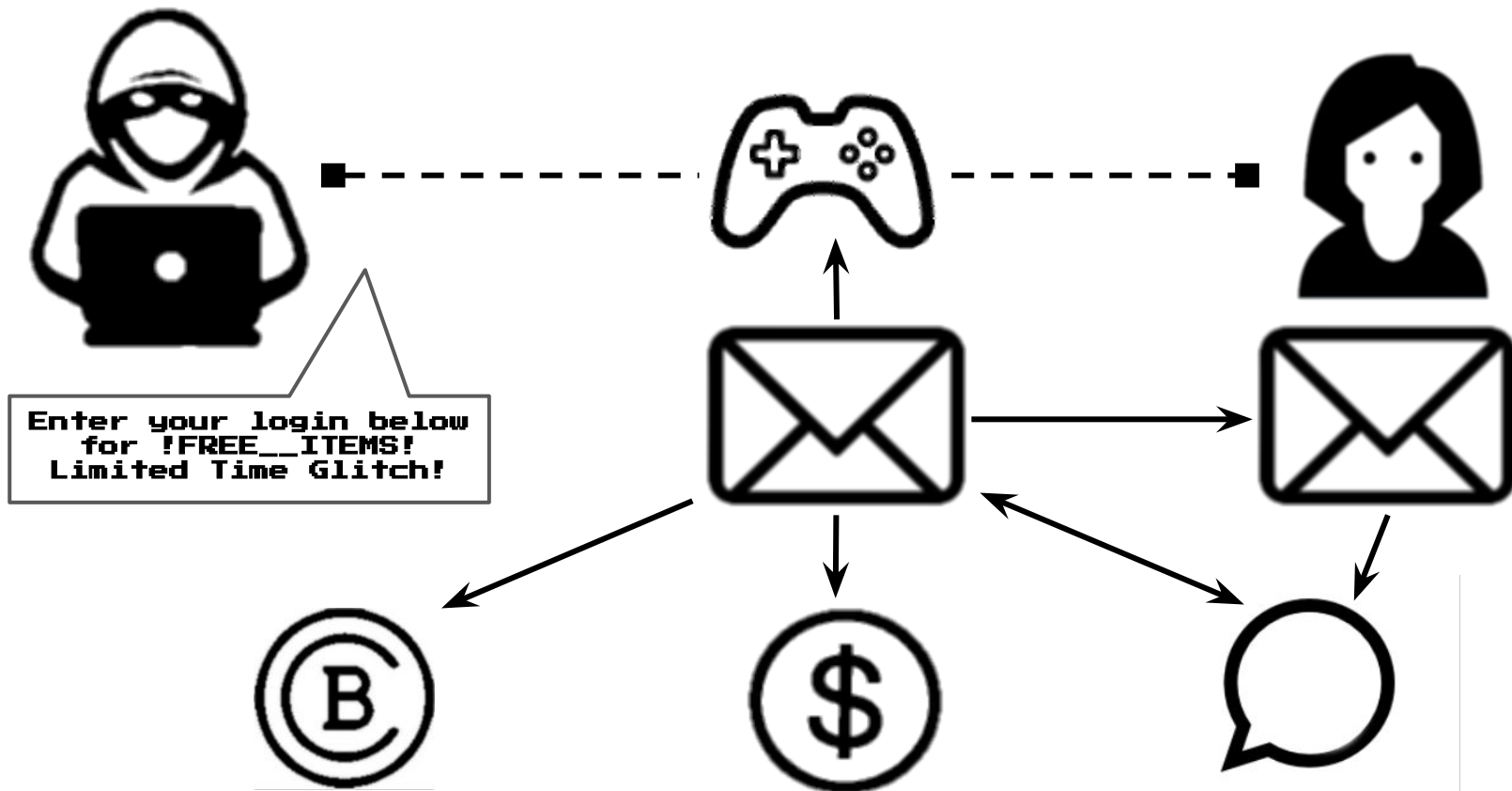
Use ethical ad-blockers and web-filtering solutions to flag and hide malicious links.



Segregate Data

- Be deliberate when setting up 2fa and recovery. Recovery credentials are a phisher's bridge to another account.
- Use several emails to back your online accounts, segregating professional, financial, and more recreational accounts.

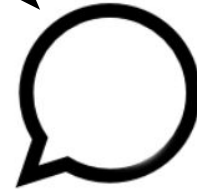




A centralized or looping account recovery chain is open to privilege escalation!



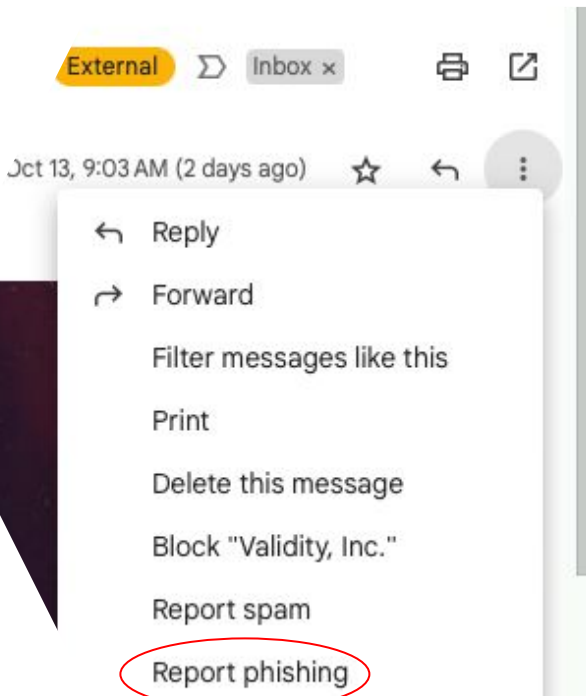
Enter your login below
for !FREE__ITEMS!
Limited Time Glitch!



A decentralized or segregated account recovery chain *can* minimize loss.

What to do with a Phishing Email

- Do not click on links
- Do not forward message to others
- Report as Phishing within email service
- Report message to company IT as applicable
- Notify affected parties
- Change passwords





Thank you!



**Baker
College**

References

Cook, S. (2022, August). Phishing statistics and facts for 2019–2023. Comparitech.com; Comparitech. <https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/>

Karimi, F. (2023, April 29). 'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping. CNN; CNN. <https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html>

Irwin, L. (2023, January 31). *The 5 most common types of phishing attack*. IT Governance Blog En. <https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack>

Phishing. NIST. (2023, April 10). <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>

Recognize and report phishing: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). <https://www.cisa.gov/secure-our-world/recognize-and-report-phishing>