

# How to Bypass Modern Phishing Detections

w/ Michael Allen



A digital illustration featuring a sleek, dark-colored fighter jet flying from the bottom left towards the top right. The jet is breaking through a large, crumpled, and exploding mass of white envelopes. Numerous individual envelopes are shown flying through the air, some trailing smoke or fire. The background is a dramatic sky with orange and yellow clouds on the left, transitioning to a deep blue with stars on the right. The overall scene conveys a sense of high speed and breakthrough.

# PUSHING THE ENVELOPE:

Lessons Learned From Another  
Year of Phishing Through the Mail



# How to Bypass Modern Phishing Detections w/ Michael Allen



# Speaker bio (Who am I?)

**Michael Allen**, OSCE, MLSE, CISSP 🙄, ...

- Pentesting and red teaming since 2014



Red Team Practice Lead at BHIS

- *Initial Access Specialist* on BHIS's ANTISOC™



I also teach:

- **Red Team Initial Access**: [WWHF Mile High](#) (Feb), [KernelCon](#) (Apr)
- **REAL Social Engineering**: [Antisyphon Red Team Summit](#) (Mar)



@Wh1t3Rh1n0 on [GitHub](#), [X](#), and [LinkedIn](#)



# Greetings once again!

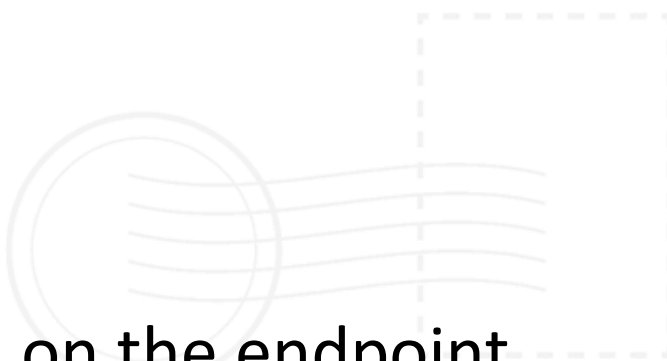


🎥 March 2024: [Greetings from the Red Team](#)



# Defensive strongholds

- Communication channels
  - Well defended:
    - Email
    - Chat messages
- Security awareness
  - Attacks expected via:
    - Email, Chat messages, SMS, Phone calls
  - Easily scrutinized:
    - Attachments, URLs

- 
- Defenses on the endpoint
    - Strong monitoring and defenses:
      - User's workstation
  - Network defenses
    - Strong monitoring and defenses:
      - Company internal network
      - Company VPN
  - External access controls
    - Affected by known, reliable attacks:
      - Multi-factor authentication
      - Geolocation



*Attack where your opponent is weakest.  
Be in the place your opponent cannot see.  
Do what your opponent does not expect.*



# Undefended / Invisible / Unexpected

- Communication channels
  - Impossible to monitor:
    - Mail to the user's home
- Security awareness
  - Attacks unexpected via:
    - Physical mail at the user's home
  - Difficult to scrutinize:
    - QR codes
- Defenses on the endpoint
  - Impossible to monitor or defend:
    - Web browser on a user's phone
- Network defenses
  - Impossible to monitor or defend:
    - User's home internet connection
    - User's mobile internet connection
- External access controls
  - Affected by known, reliable attacks:
    - Multi-factor authentication
    - Geolocation



Contoso Ltd.  
456 Elm Street  
Spearfish, SD 57783



Alice Smith  
123 Main St.  
Albuquerque, NM 87107

# YOU ARE AMAZING

---





Dear Alice,

It is my pleasure to inform you that a teammate recently nominated you for a peer recognition award.

On behalf of our Contoso family, please accept this \$50 Amazon gift card as a small token of our appreciation for you and all the hard work you do.

Sincerely,  
Carol Roberts  
Chief Human Resources Officer

---

Gift card instructions: Use your phone to scan the QR code on the left, and sign in with your Contoso email to claim your electronic gift card.

# MFA-enabled credential harvesting

7:55 76%

login-contoso.com

Microsoft

## Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back Next

Microsoft

alice@contoso.com

## Enter code

123 Enter the code displayed in the authenticator app on your mobile device

Code

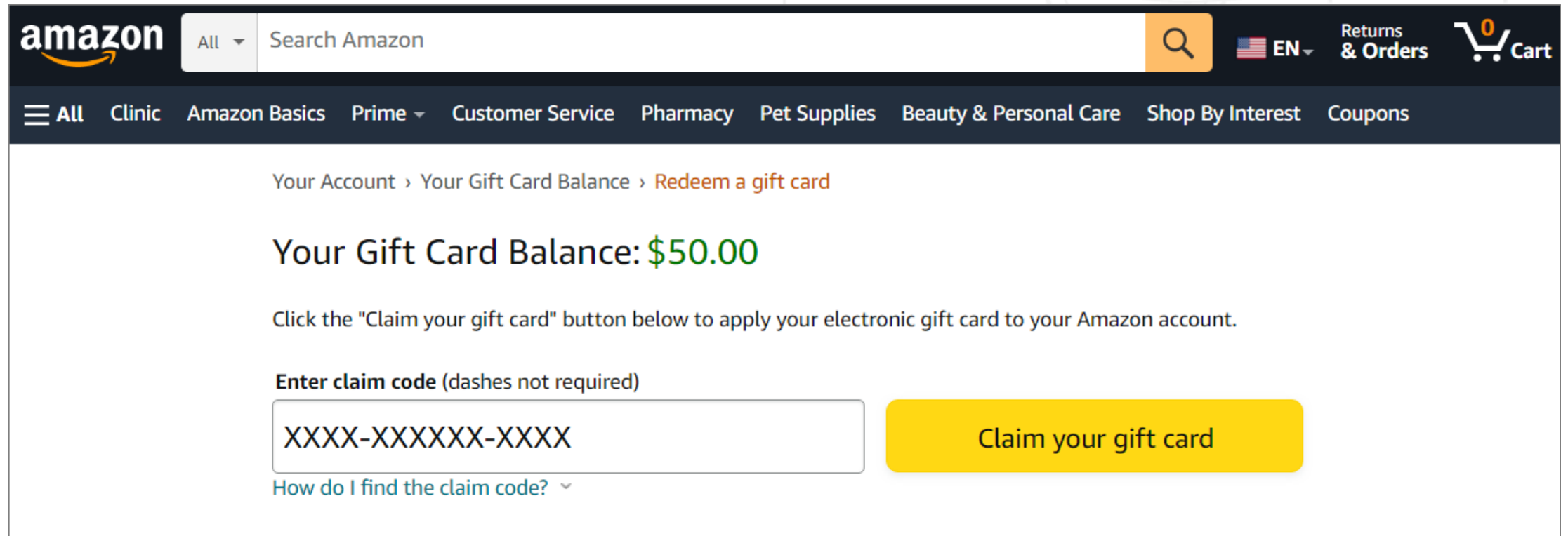


Evilginx 3: <https://github.com/kgretzky/evilginx2>





# Reward with a REAL gift card



amazon All Search Amazon

EN Returns & Orders Cart

All Clinic Amazon Basics Prime Customer Service Pharmacy Pet Supplies Beauty & Personal Care Shop By Interest Coupons

Your Account > Your Gift Card Balance > Redeem a gift card

Your Gift Card Balance: **\$50.00**

Click the "Claim your gift card" button below to apply your electronic gift card to your Amazon account.

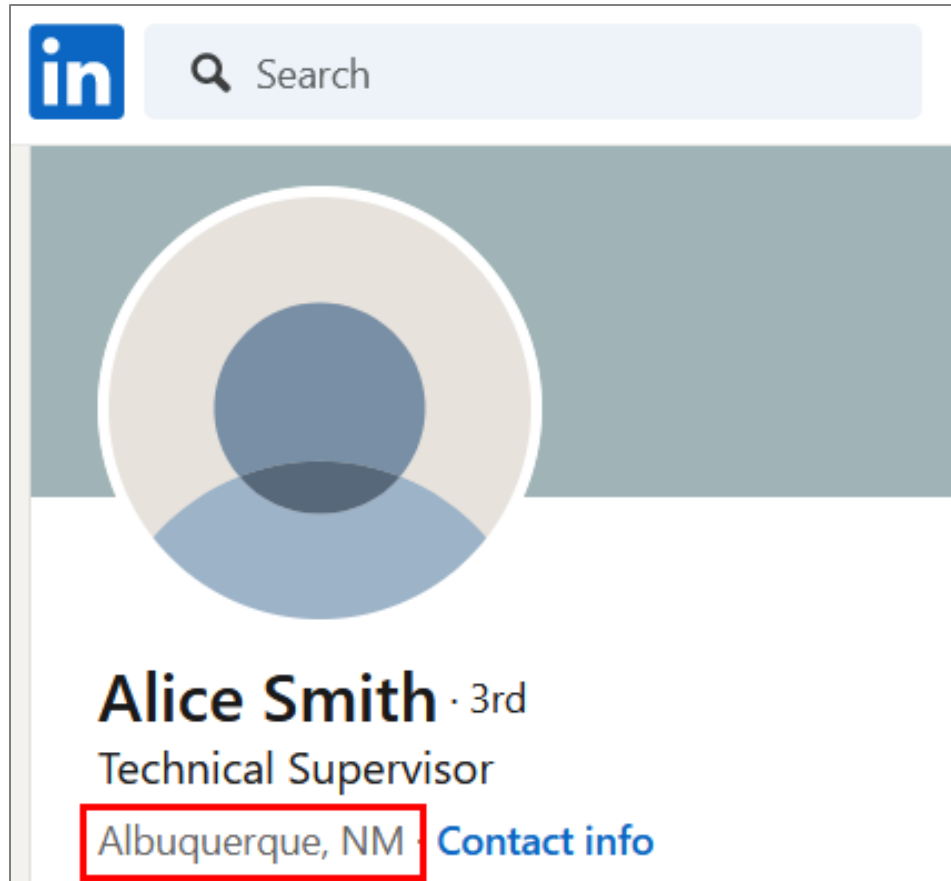
Enter claim code (dashes not required)

XXXX-XXXXXX-XXXX

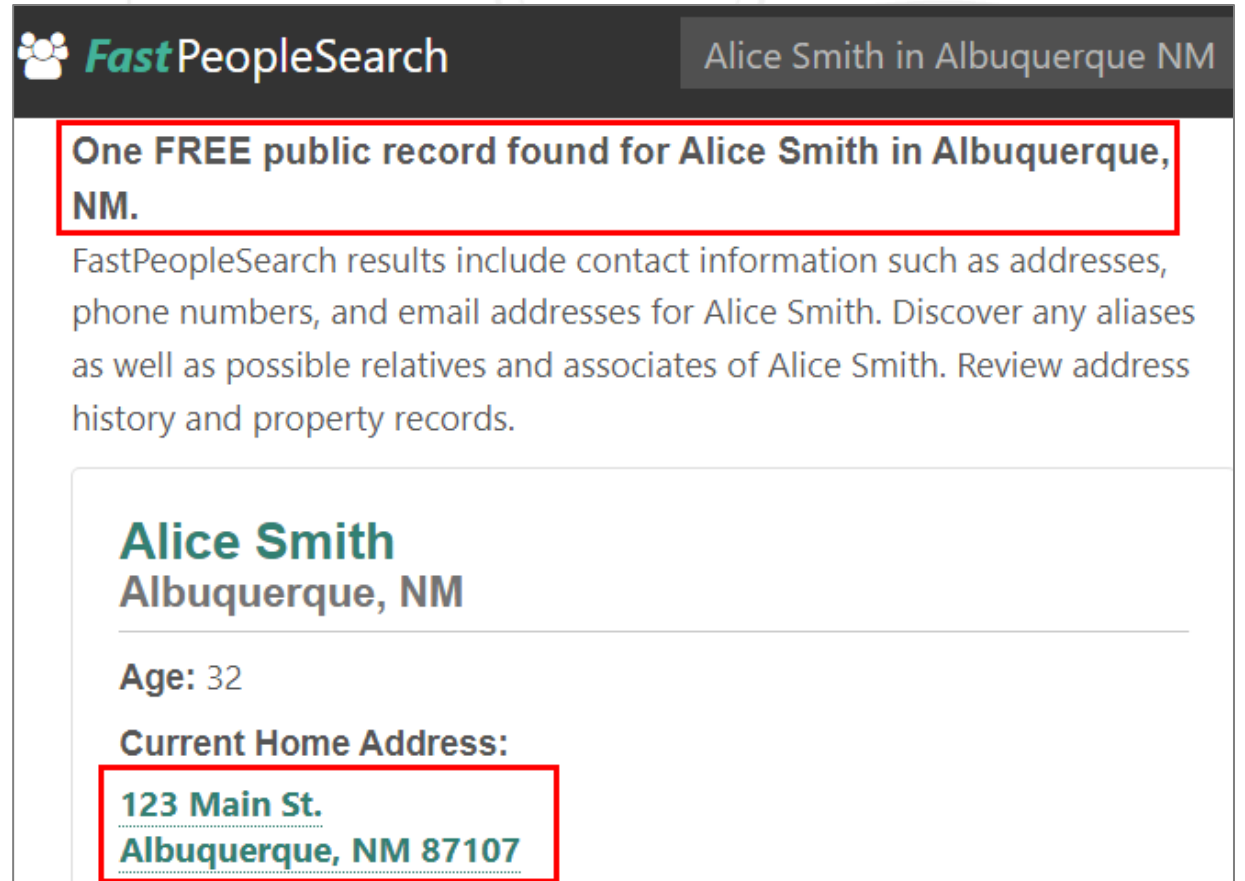
How do I find the claim code? ▾

Claim your gift card

# Find the address

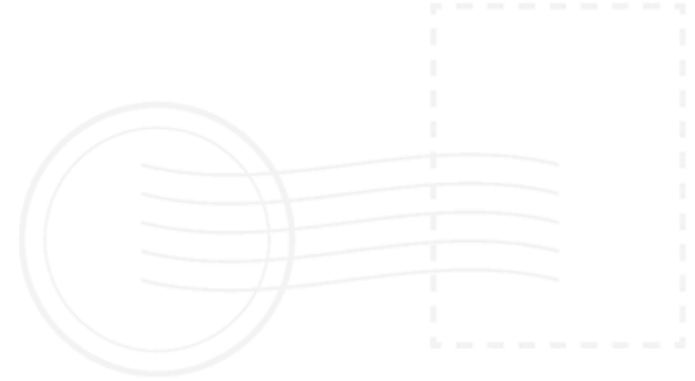


LinkedIn profile of Alice Smith. The profile shows a blue header with the LinkedIn logo and a search bar. Below the header is a large circular profile picture. Under the picture, the name "Alice Smith" is displayed in bold, followed by "· 3rd" and "Technical Supervisor". At the bottom, the location "Albuquerque, NM" is highlighted with a red box, and a blue "Contact info" link is visible.



FastPeopleSearch results for Alice Smith in Albuquerque, NM. The search bar at the top shows "Alice Smith in Albuquerque NM". A red box highlights the text: "One FREE public record found for Alice Smith in Albuquerque, NM." Below this, a paragraph states: "FastPeopleSearch results include contact information such as addresses, phone numbers, and email addresses for Alice Smith. Discover any aliases as well as possible relatives and associates of Alice Smith. Review address history and property records." A section titled "Alice Smith" and "Albuquerque, NM" follows. Below this, "Age: 32" is listed. Under "Current Home Address:", the address "123 Main St. Albuquerque, NM 87107" is highlighted with a red box.

# Lessons learned



---

---

---

---

---

---



# Lessons learned

1. **Don't order the Amazon gift cards from your personal account.** 😊
  - *Even if you order physical or "Print at Home" cards.*

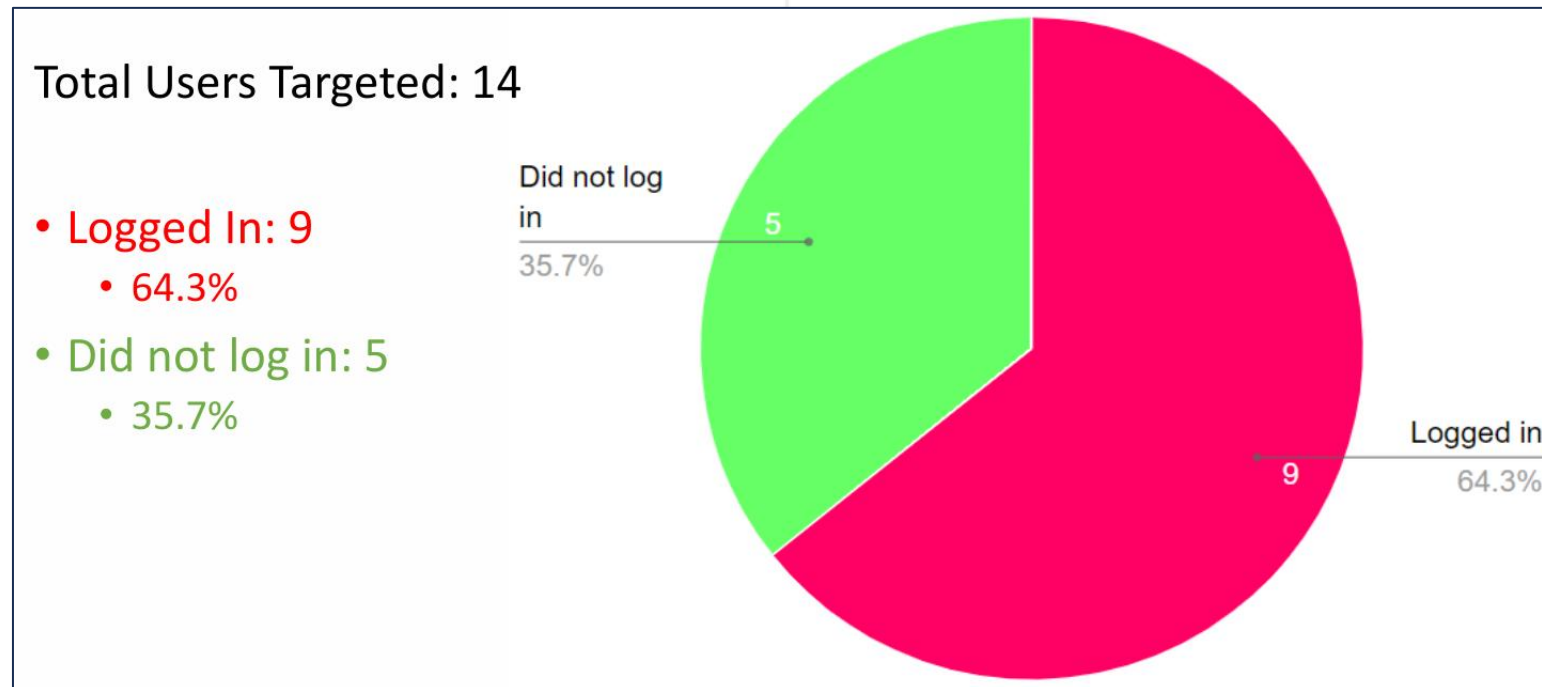




# Lessons learned

## 2. Don't send more than about 10 postcards per organization.

- The *majority* of targeted users log in.



# Lessons learned

## 3. People *really* want that Amazon gift card.

How could we tell?



---

---

---

---

---

---

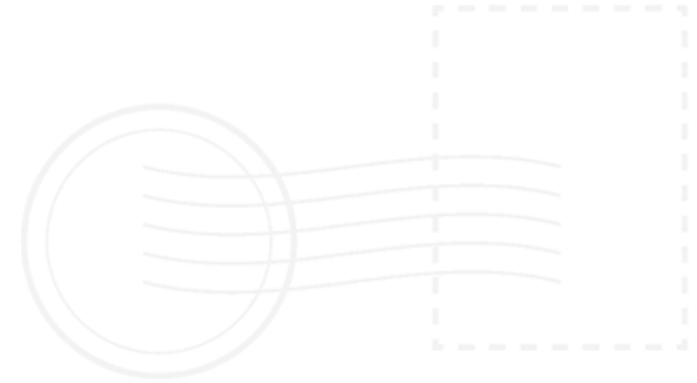


# Lessons learned

## 3. People *really* want that Amazon gift card.

How could we tell?

1. Not just the “technically unsophisticated” users.



---

---

---

---

---

---



# Lessons learned

## 3. People *really* want that Amazon gift card.

How could we tell?

1. Not just the “technically unsophisticated” users.
2. Log-ins from users who were out on vacation.
  - 🎥 Oct. 2024: [Adversary in the Middle \(AitM\): Post-Exploitation](#)





# Lessons learned

## 3. People *really* want that Amazon gift card.

How could we tell?

1. Not just the “technically unsophisticated” users.
2. Log-ins from users who were out on vacation.
3. Multiple log-ins from the same person.
  - Some users tried logging in once, ***changed their passwords***, and then tried logging in again with the new password.



# Lessons learned

## 3. People *really* want that Amazon gift card.

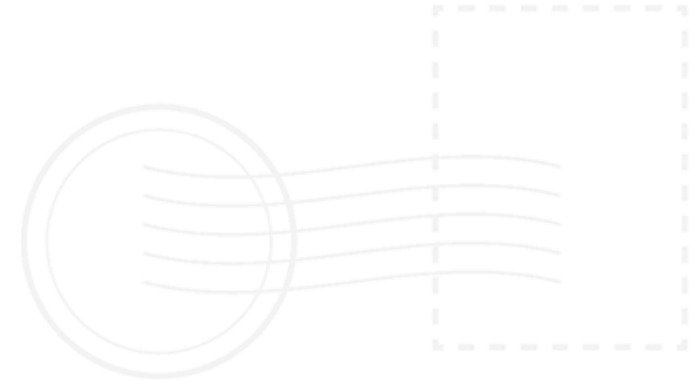
How could we tell?

1. Not just the “technically unsophisticated” users.
2. Log-ins from users who were out on vacation.
3. Multiple log-ins from the same person.
4. Log-ins continued ***two months*** after the campaign end. 🤖
  - ***Even after organizations told employees not to!***



# Why such a strong response?

- \$50 Amazon Gift Card
  - **Enticing** amount of value for most people.
- Authority
  - Signed by the head of HR.
  - Branded with the company logo.
- Looked the part
  - No misspelled words, grammar errors, etc.
  - Perfect clone of company login portal.
- *Triggered an emotional reaction*





# Emotional hijacking





# Emotional hijacking

- A person operates *logically* or *emotionally* at any given time. Not both.
- Emotional responses are *faster* than logical.
  - Why? Evolution.
  - “Is that a stick or a snake?”
- Emotional Hijacking
  1. An event triggers a sudden, **emotional** response.
  2. Your *emotional* brain (amygdala) **overrides** your *logical* brain (prefrontal cortex).



Image credit: [GolfMagic](#)



# What happens when they get the postcard?

- It's Saturday...
  - Finally, some time to relax and recover.
  - *Not* in a work state of mind.
- They get up to check the mail...
  - What's this? Mail from work?
    - *"What do they want?"*
- Open the envelope...
- ***"Peer Recognition Award"?! 🤔***
  - ***"appreciation for all the hard work you do"?! 😊❤️***
  - ***\$50 Amazon Gift Card! 💰 🌟 🎉***



# What happens *next*?

- **They tell someone.**
- How are they feeling now?
  - Proud
  - Validated
  - Appreciated
- They ***want to believe***.
- They're ***invested***.
- Questioning the ruse now would mean *maybe they didn't really deserve that award.*



# How to defend?



---

---

---

---

---

---



# How to defend?

1. Secure the humans: **Security Awareness Training**
2. Secure the machines: **Technical Defenses**



---

---

---

---

---

---



# First line of defense: *Security Awareness*

- Why?
  - Creative attackers will ***always*** be able to ***avoid*** technical security controls if they can imagine a situation you have not considered.
- Effective security awareness training
  1. Concept / principal focused
    - Resilient to novel, future attacks
  2. Regular practice + Multiple channels
    - Email, phone, SMS, Teams, LinkedIn, snail mail, USB drops, etc.
  3. Reward desired behavior – *Positive reinforcement*





# Combating emotional hijacking

1. Notice any time you have an emotional response. (Takes practice.)
  - This is your warning sign.
2. **STOP! Slow down and think** about what is happening.
  1. Is it *likely* that the situation is what it appears to be?
  2. Are you about to take an action that *could* possibly be dangerous?
    - Logging into a website.
    - Opening a file.
    - Making a financial transaction.
    - Disclosing information.
  3. Is there a third party who can *verify* the situation?
    - A third party that you select.



# Technical defenses

Either of these will **stop** current Adversary-in-the-Middle attacks:

- Switch to [phishing-resistant MFA](#) such as FIDO2/U2F/WebAuthn.
- Allow logins ***only*** from the internal network or VPN.

If too costly, consider applying to highly-privileged users first.

Others will ***sometimes detect*** Adversary-in-the-Middle attacks:



- Impossible travel alerts.
- Alert on any logins from suspicious IP addresses (CSPs, TOR, VPNs, etc.), or devices/browsers that the user has not logged in from before.
- [Add and monitor canary tokens on the login portal.](#)



# Thank you for listening!



Want to learn more?

-  [\*\*REAL Social Engineering\*\*](#)
  - Learn the fundamental skills for exploiting human psychology used on *real* social engineering penetration tests.
-  [\*\*Red Team Initial Access\*\*](#)
  - The *top, up-to-date* attacks we use to breach environments on red team exercises.
  - Includes the full attack chain I described in this talk, *plus more!*

Follow me, Michael Allen (@Wh1t3Rh1n0) on:

- [X](#)
- [LinkedIn](#)
- [GitHub](#)

