RSAC | 2025 Conference

Many Voices.
One Community.

SESSION ID: HUM-W09

Greetings from the Red Team!

Michael Allen

Senior Security Analyst / Red Team Practice Lead
Black Hills Information Security
https://linkedin.com/in/wh1t3rh1n0

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Hurdles to modern hacking

The “good old days”…

- Email defenses were unsophisticated or nonexistent.
- Antivirus products weren’t very good or weren’t present at all.
- No such thing as Endpoint Detection and Response (EDR).
- End users had never heard of “phishing” or “social engineering”.
- Limited knowledge of their own network topology, inventory, and exposure.

Defenders were operating blind.

Common defenses today

- **Communication channels**
  - Email – filtered based on:
    - Domain age and reputation
    - Email security standards (SPF, DKIM)
    - Message content
  - Chat messages
    - Restricted to internal users only
- **Security awareness**
  - Users suspicious of email, chat messages, SMS, phone calls
  - Users trained to scrutinize attachments and URLs
- **Defenses on the endpoint**
  - Advanced EDR/antivirus
  - Rapid response and isolation following a single alert
- **Network defenses**
  - Egress controls
  - Traffic decryption and inspection
  - Web traffic filtering
- **External access controls**
  - Multi-factor authentication
  - Geolocation

Going head-to-head is a waste of time

Thinking outside the box

Attack where your opponent is weakest.

Be in the place your opponent cannot see.

Do what your opponent does not expect.

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

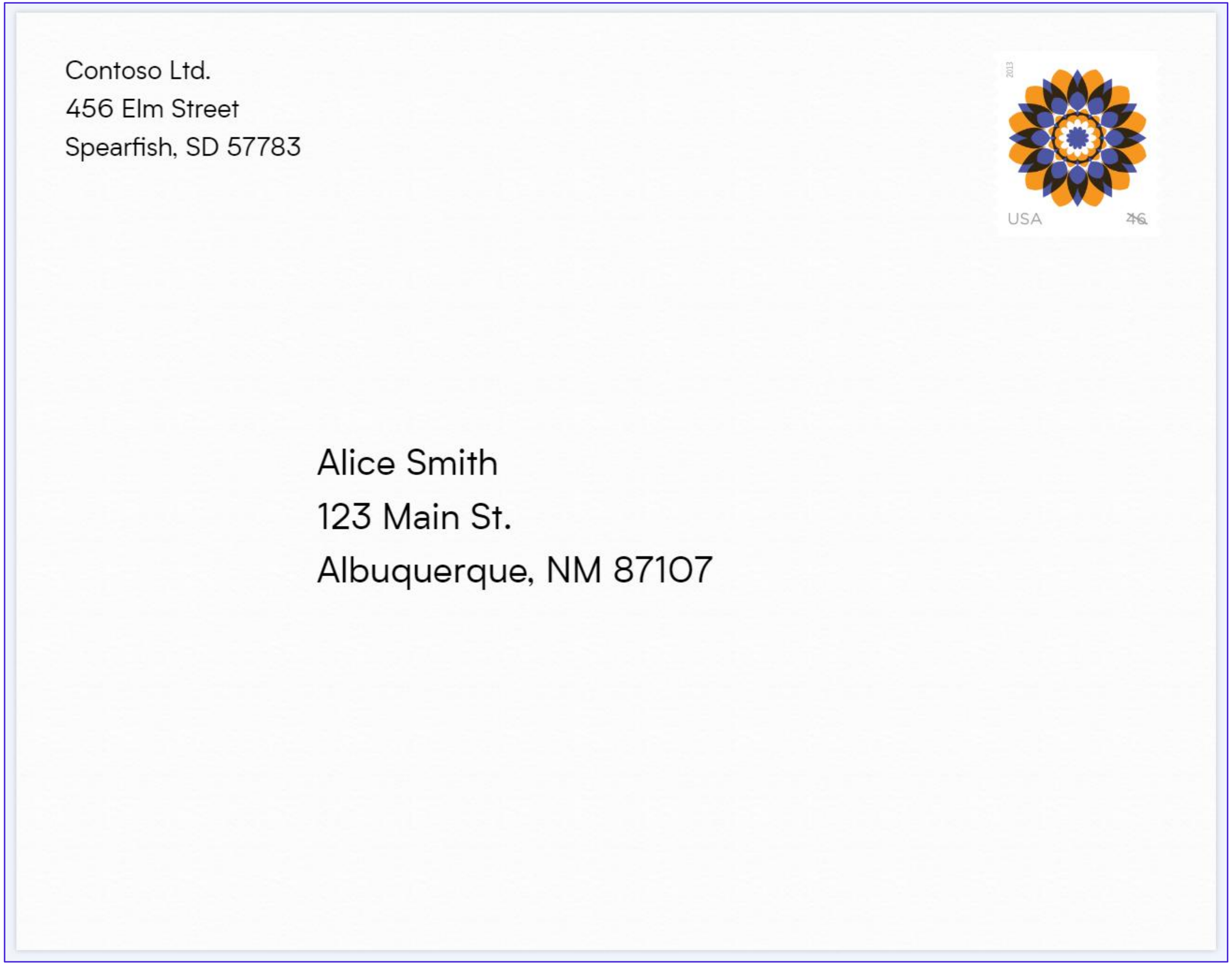
Undefended / Invisible / Unexpected

- **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

RSAC | 2025 Conference

A new attack is born

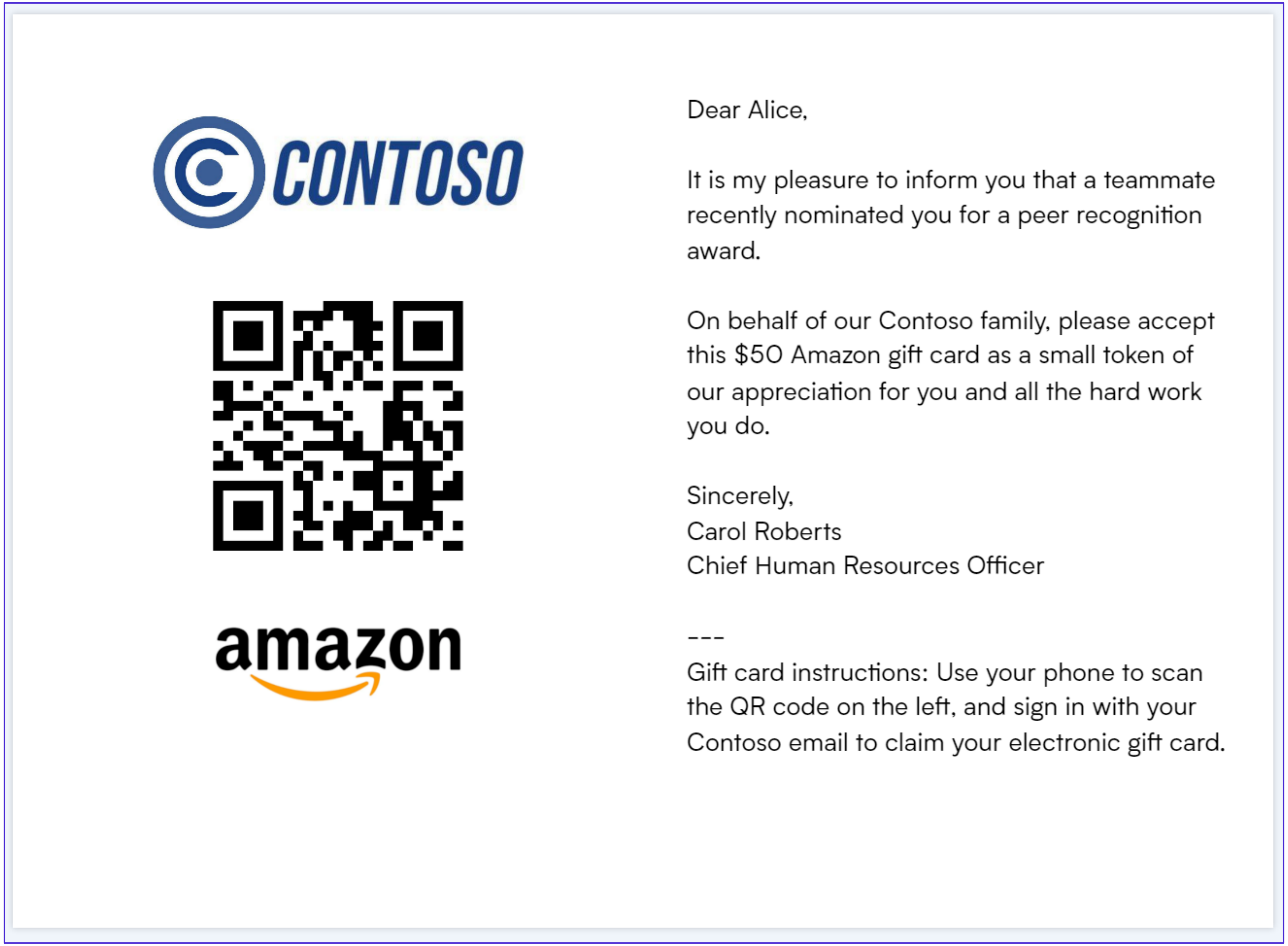
Many Voices.
One Community.



Contoso Ltd.
456 Elm Street
Spearfish, SD 57783

Alice Smith
123 Main St.
Albuquerque, NM 87107

YOU ARE
AMAZING
CONTOSO


CONTOSO
amazon

Dear Alice,

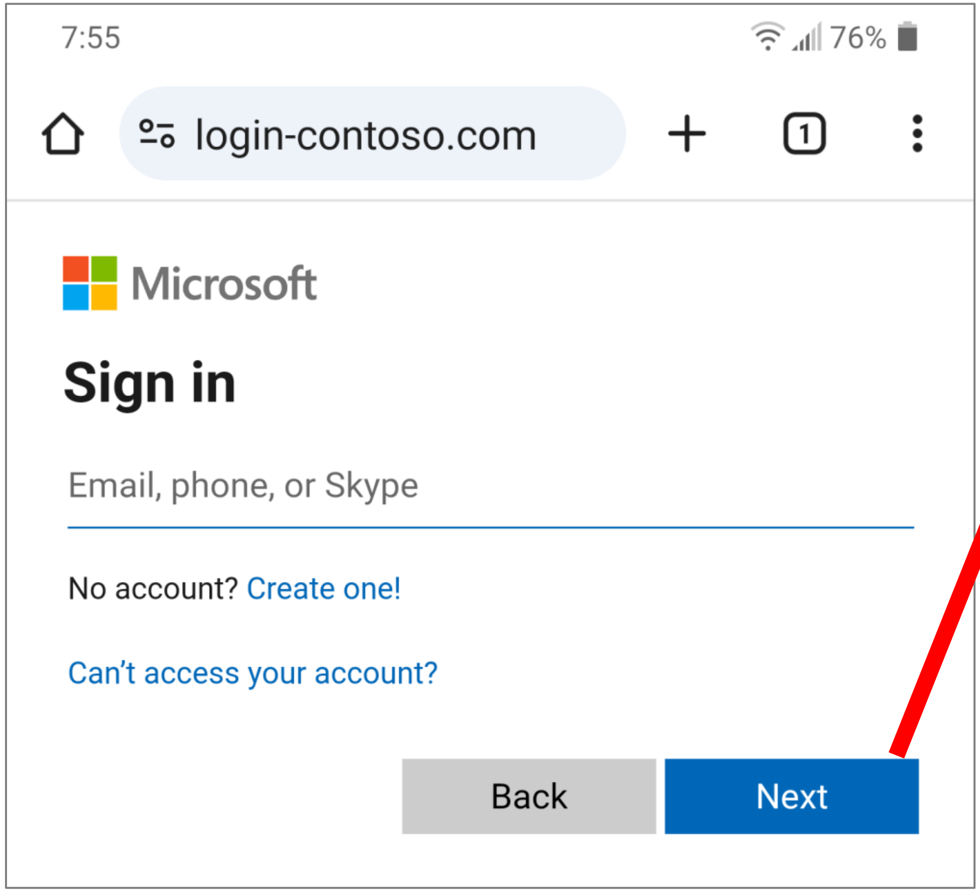
It is my pleasure to inform you that a teammate recently nominated you for a peer recognition award.

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.

“Adversary-in-the-Middle” phishing



7:55 76%

login-contoso.com

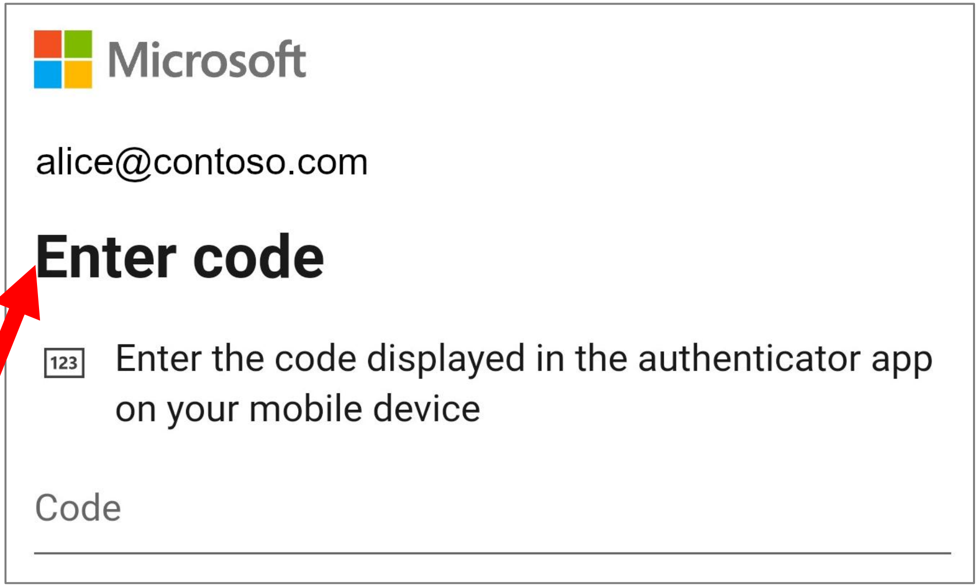
Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can’t access your account?



Microsoft

alice@contoso.com

Enter code

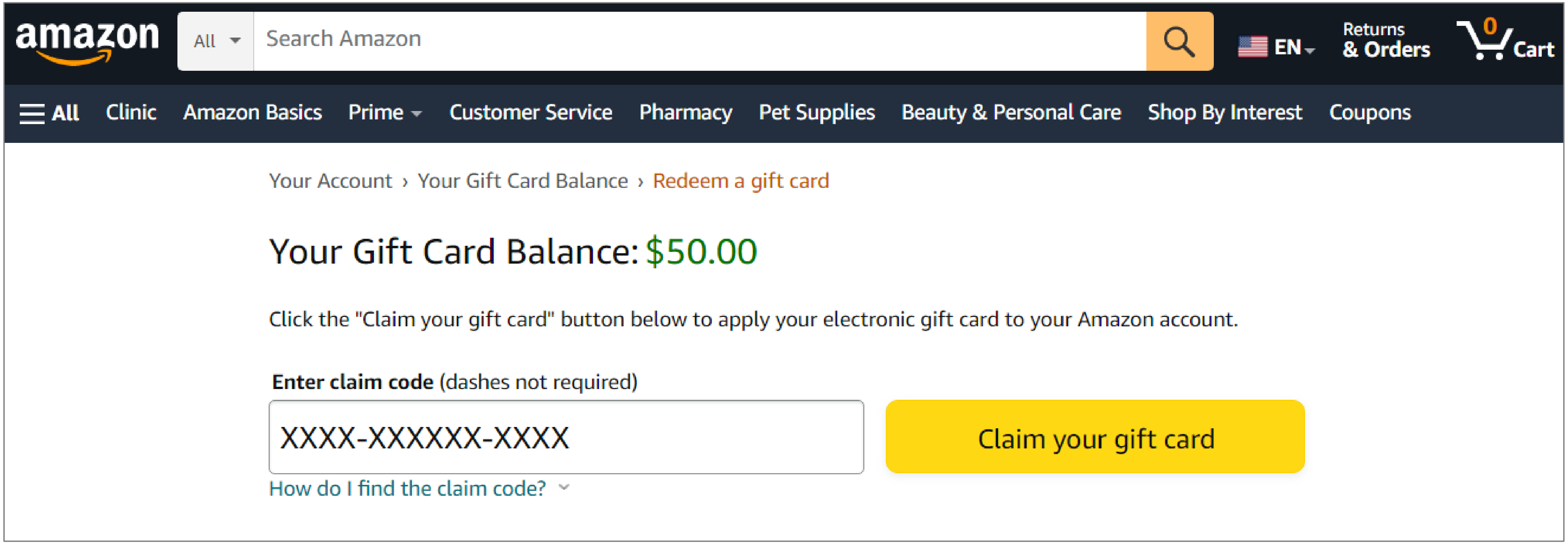
Enter the code displayed in the authenticator app on your mobile device

Code

evilginx.

Evilginx: https://github.com/kgretzky/evilginx2

Reward with a ***REAL*** gift card



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.

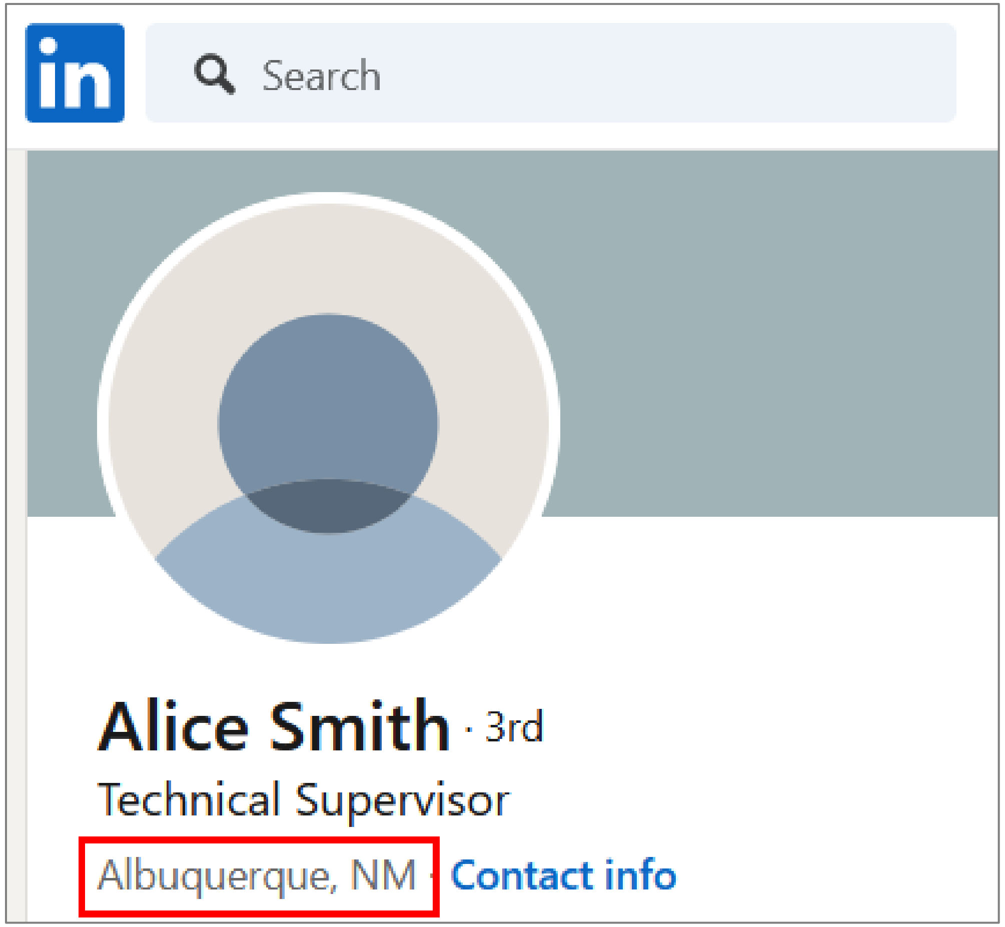
Enter claim code (dashes not required)

XXXX-XXXXXX-XXXX

Claim your gift card

How do I find the claim code?

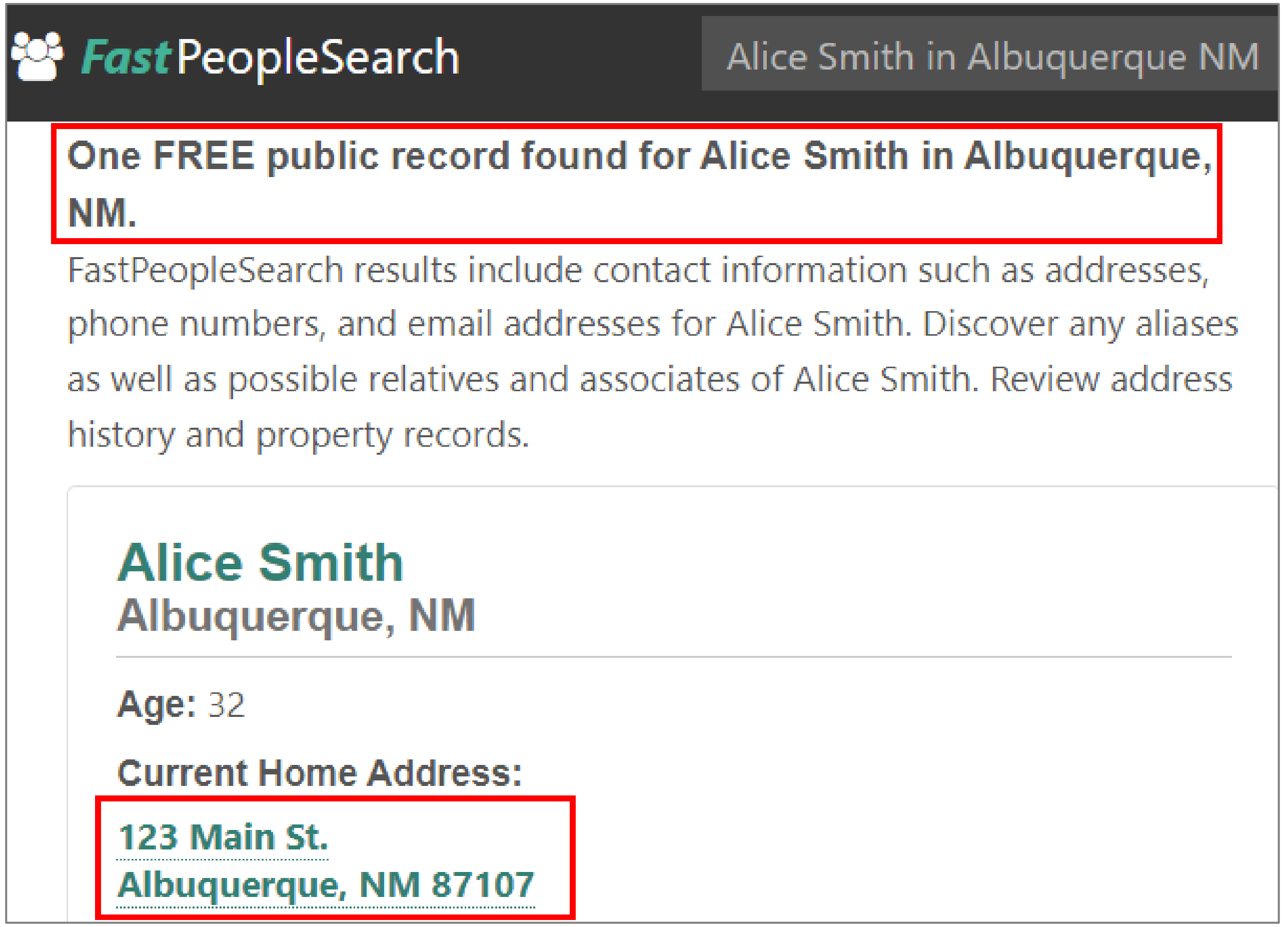
Find the address



Alice Smith · 3rd

Technical Supervisor

Albuquerque, NM · Contact info



One FREE public record found for Alice Smith in Albuquerque, NM.

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.

Alice Smith
Albuquerque, NM

Age: 32

Current Home Address:

123 Main St.
Albuquerque, NM 87107

How to defend?

Many Voices.
One Community.

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 that you have not considered.

- Effective security awareness training
  1. Concept & principle focused
     - Resilient to novel, future attacks
  2. Regular practice + Multiple channels
     - Email, phone, SMS, Microsoft Teams, LinkedIn, physical mail…
  3. *Reward* desired behavior – *Positive reinforcement*

Second line of defense: **Technical Defenses**

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

1. Switch to phishing-resistant MFA such as FIDO2 / U2F / WebAuthn.
2. Allow logins ***only*** from the internal network or VPN.

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

❌ Other solutions ***only sometimes detect*** AitM attacks:

- Impossible travel alerts.
- Alert on logins from suspicious IPs (TOR, VPN, CSP) or browsers.
- Add and monitor canary tokens on the login portal.

RSAC 2025 Conference

Apply what you learned here today

Many Voices.
One Community.

Apply What You Learned (Attackers😈)

1. On your next project: **Try phishing with postcards!**
   - This is by far the most effective attack I have seen in the last decade.
   - *Let's make postcard phishing so common* ***that it doesn't work anymore!***
2. On your future projects: **Always Be Cheating**™
   - Never go head-to-head. *Always fight dirty.*

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

Apply What You Learned (Defenders 🛡️)

1. Review your organization’s security awareness training program.
   - Does it teach *principles* that apply to a *variety* of attacks?
   - Are employees tested over a *variety* of communication channels?
   - Does it *reward* desired behaviors?
2. Test your MFA for vulnerability to Adversary-in-the-Middle.
   - 🎥 “*How to Test Adversary in the Middle Without Hacking Tools*”
3. Short-term goal: Disallow weak MFA methods on admin accounts.
4. Long-term goal: Transition all users to phishing-resistant MFA.

Thank You!

For more information:

📢 **Follow Michael Allen: @Wh1t3Rh1n0 on LinkedIn & X**

🧑‍🏫 **Learn *Red Team Initial Access*: initial-access.com/rsa**