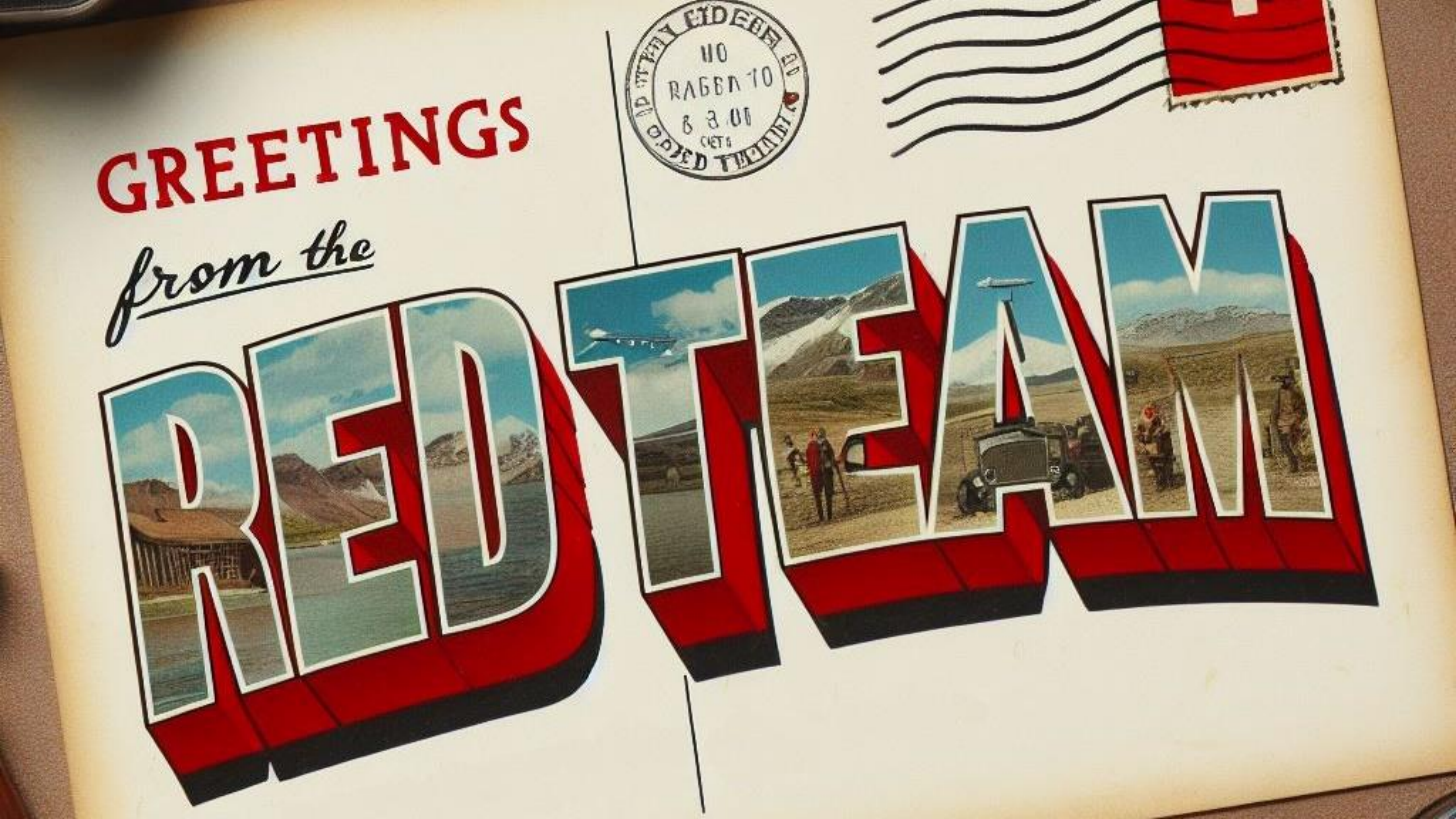


GREETINGS
from the
RED TEAM
NO
RAGEN 70
6 3.06
CETS

Speaker bio (Who am I?)

Michael Allen (@Wh1t3Rh1n0)

- Pentesting and red teaming for 9+ years
- Red team lead at BHIS
  - Special interest in Initial Access
- Creator and instructor of "Red Team Initial Access"
  - Focus on ***immediately actionable*** training
  - June 20-21 on AntiSyphonTraining.com

*Thanks to **Joseph Kingstone** on the BHIS Red Team for input & testing.*

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 (not an exhaustive list)

- 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

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

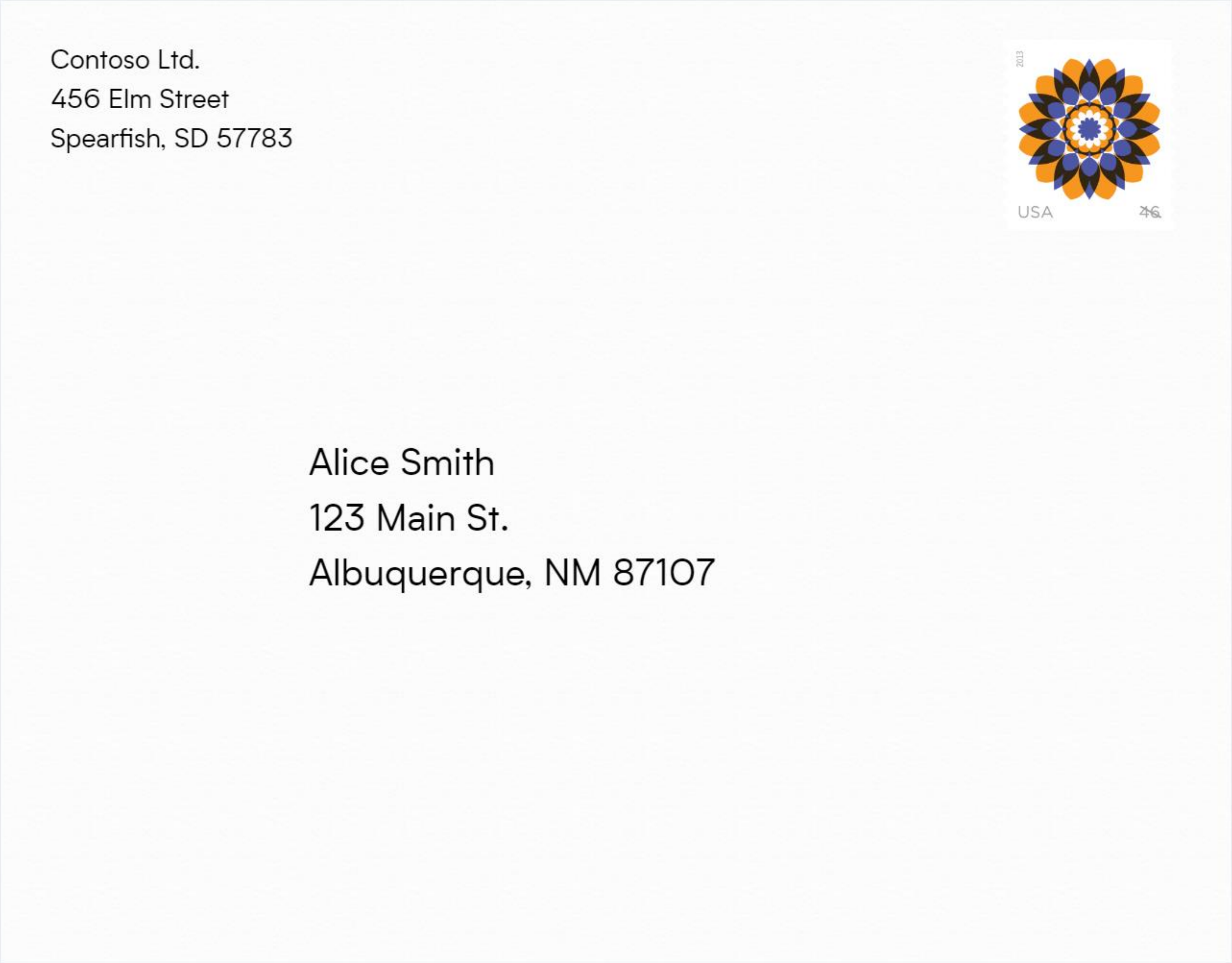
- Defenses on the endpoint
  - Strong monitoring and defenses:
    - User's workstation
- Network defenses
  - Strong monitoring and defenses:
    - Company internal network
    - Company VPN
- External access controls
  - Affected by known, reliable attacks:
    - Multi-factor authentication
    - Geolocation

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

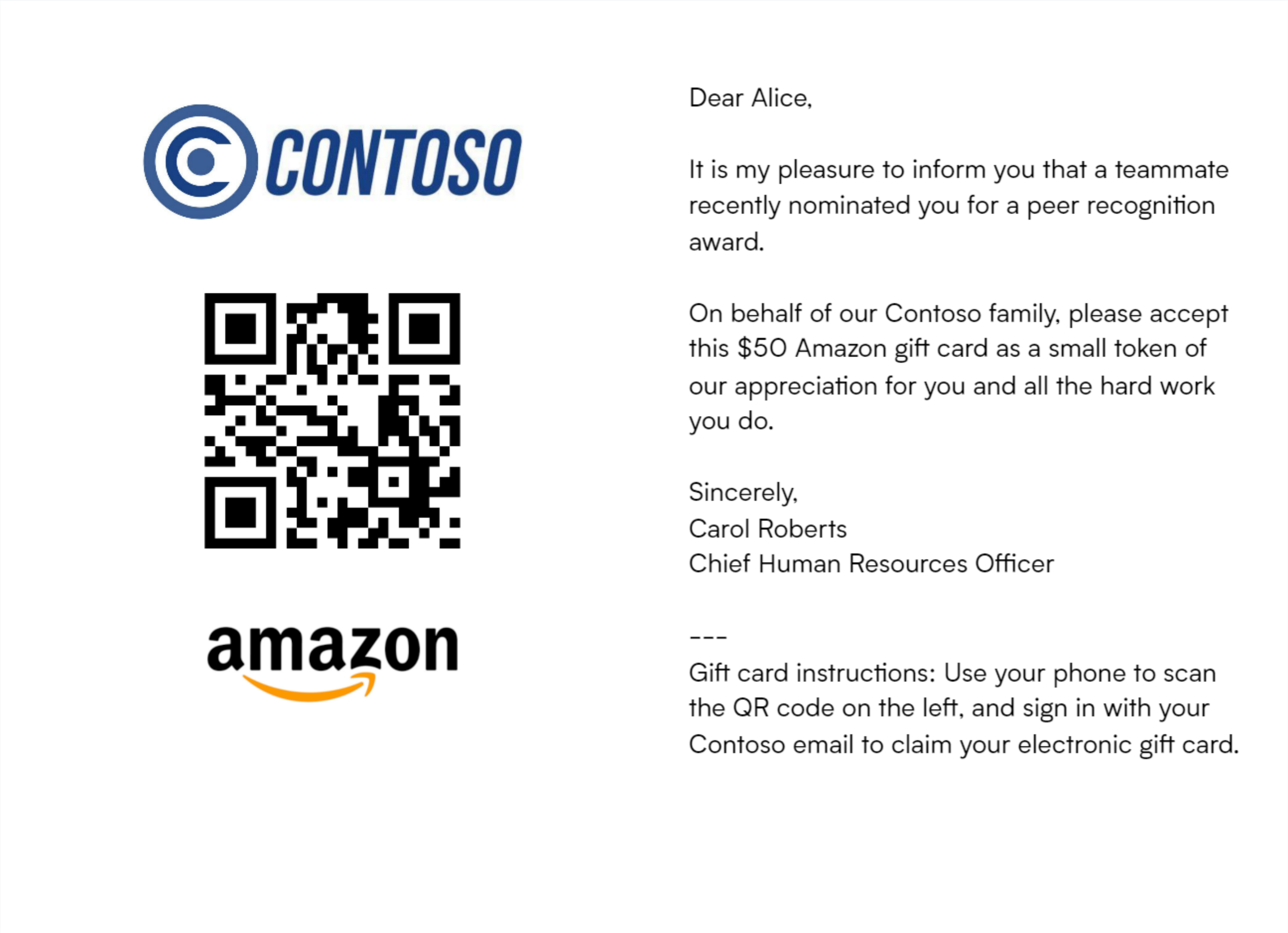
A new attack is born



Contoso Ltd.
456 Elm Street
Spearfish, SD 57783

Alice Smith
123 Main St.
Albuquerque, NM 87107

YOU ARE
AMAZING
CONTOSO


CONTOSO
amazon

Dear Alice,

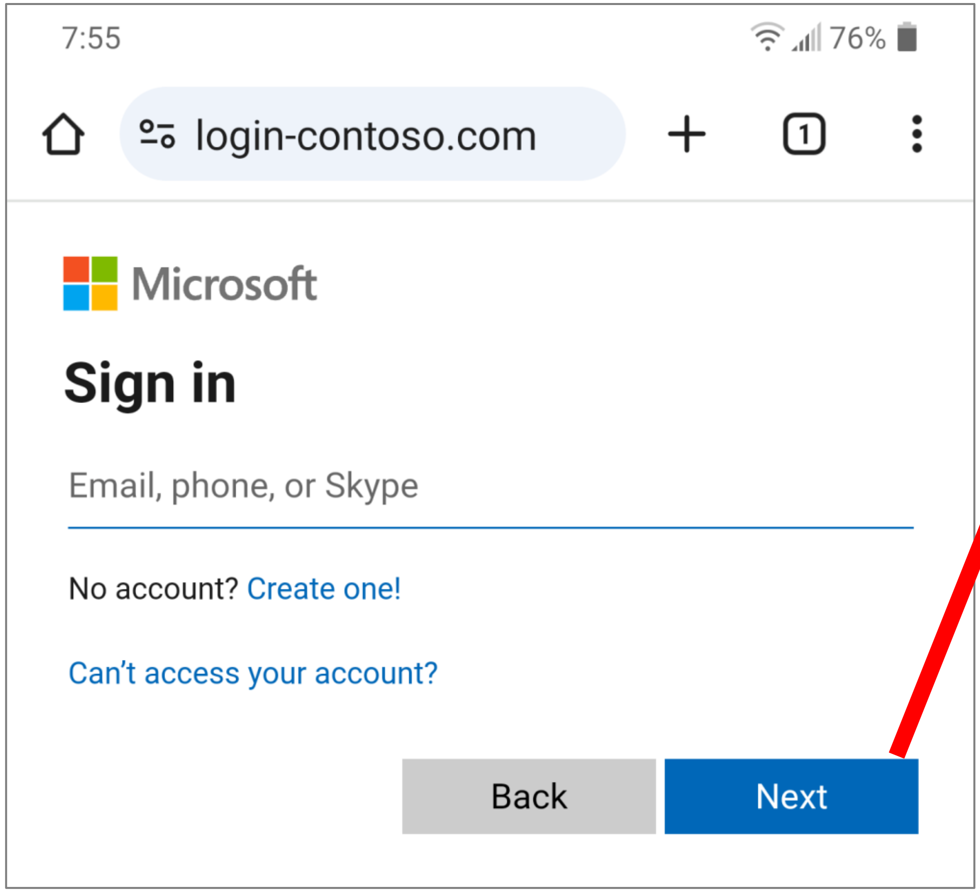
It is my pleasure to inform you that a teammate recently nominated you for a peer recognition award.

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.

MFA-enabled credential harvesting



7:55 76%

login-contoso.com

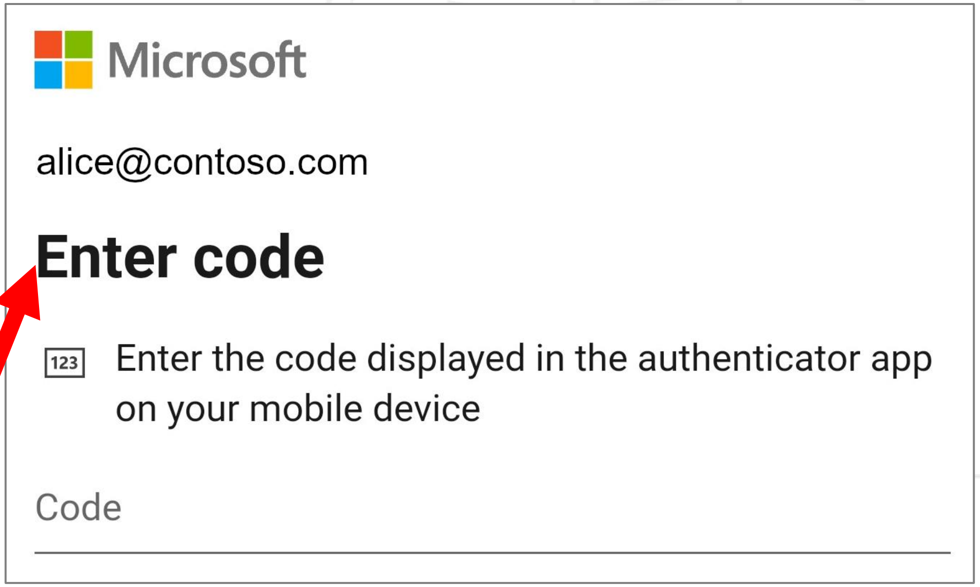
Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can’t access your account?



Microsoft

alice@contoso.com

Enter code

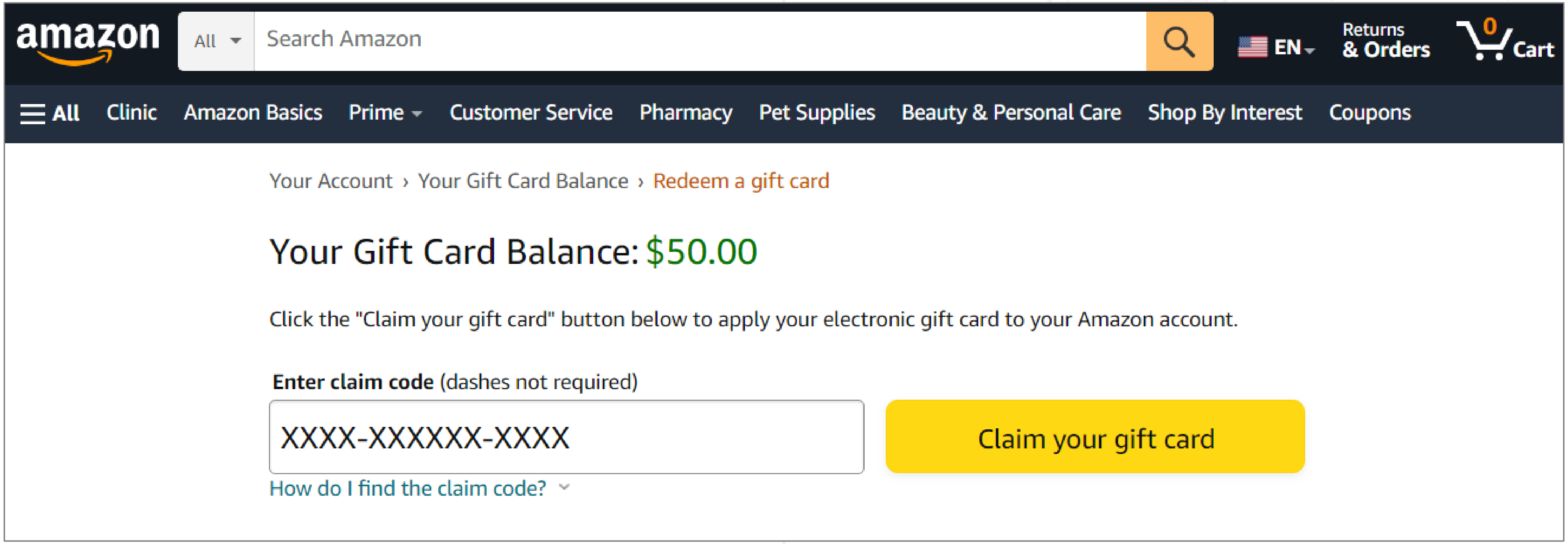
Enter the code displayed in the authenticator app on your mobile device

Code

evilginx.

Evilginx 3: 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.

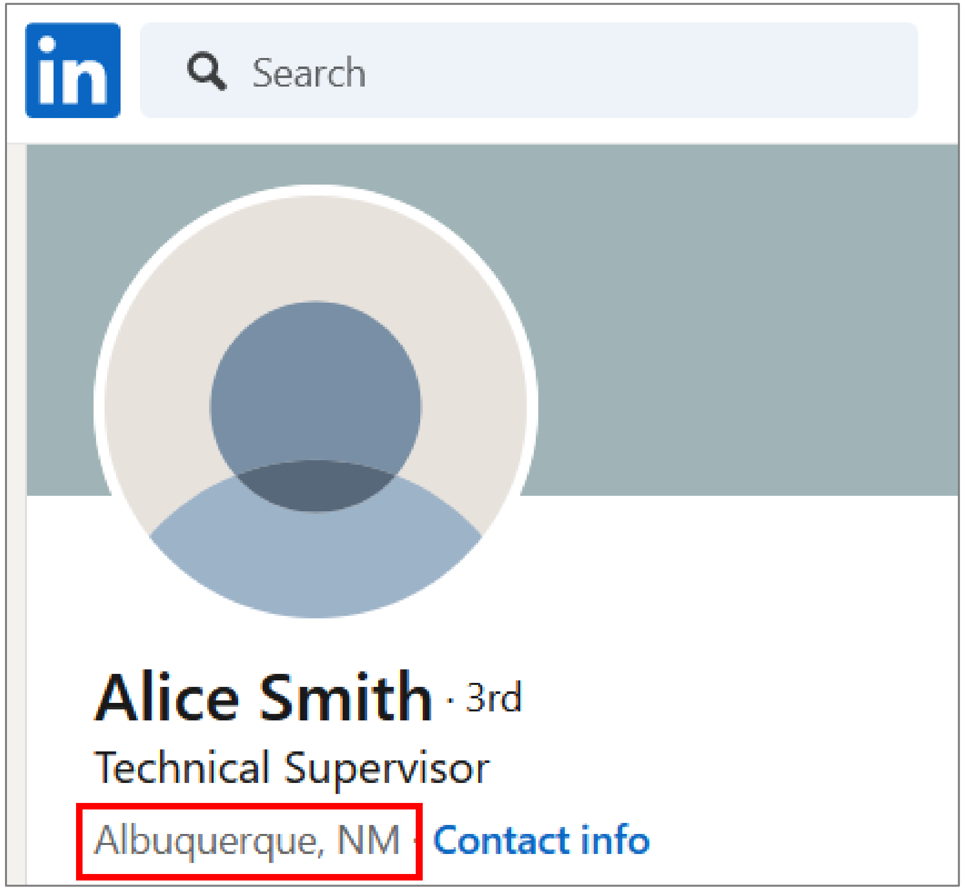
Enter claim code (dashes not required)

XXXX-XXXXXX-XXXX

Claim your gift card

How do I find the claim code?

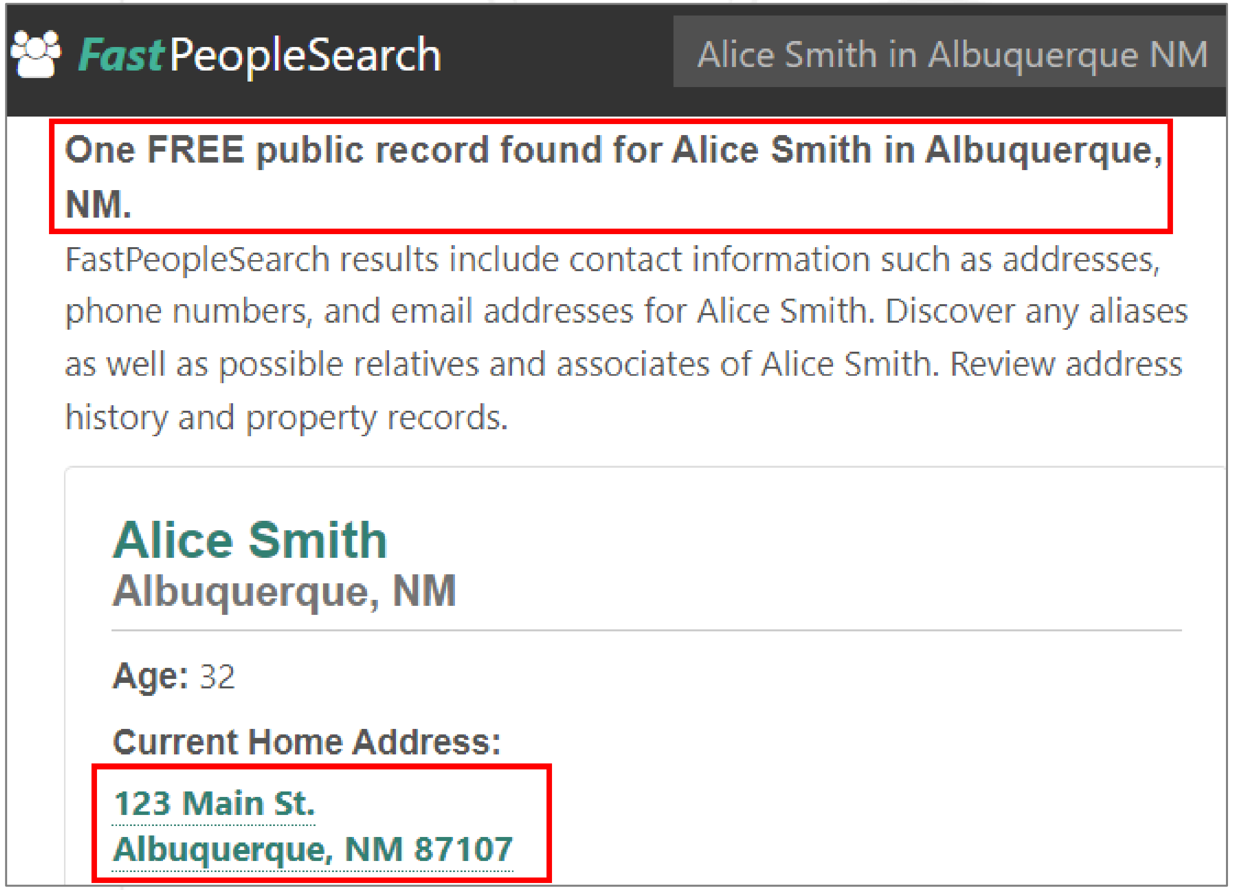
Find the address



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?

Some defenses (not a comprehensive list)

- Security Awareness Training
  - Concept / principal focused
    - Resilient to novel, future attacks
  - Regular practice + Multiple channels
    - Email, phone, SMS, Teams, LinkedIn, snail mail, USB drops, etc.
- Allow login ONLY from internal network/VPN
  - “Control the battlefield”
- Phishing-Resistant MFA
  - Example: FIDO 2

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
  - Strong monitoring and defenses:
    - Company internal network
    - Company VPN
- External access controls
  - Strong monitoring and defenses:
    - External logins disallowed
  - Vulnerabilities moot:
    - Multi-factor authentication
    - Geolocation

Some defenses (not a comprehensive list)

- Security Awareness Training
  - Concept / principal focused
    - Resilient to novel, future attacks
  - Regular practice + Multiple channels
    - Email, phone, SMS, Teams, LinkedIn, snail mail, USB drops, etc.
- Allow login ONLY from internal network/VPN
  - “Control the battlefield”
- Phishing-Resistant MFA
  - Example: FIDO 2

Thank you for listening!

Want to learn more?

- “Red Team Initial Access” class
  - June 20-21 on AntiSyphonTraining.com
- Follow me: @Wh1t3Rh1n0