Wireframe Purpose

- This will be part of a living threat modeling library to reference as we characterize bad actors, map out actions, and recommend account security measures
- This will be graphically organized into a nested/cross-linked flowchart or matrix

1. Each node is a point of vulnerability/recommendation of control we can potentially detect/monitor directly or indirectly
2. Each sub-node is an attack vector

Tag recommendation points In our control (IC), Out of our control (OC), Can influence (I)

Account Takeover Attack Tree for <company>

Credential Theft

Malware and Spyware (Indirectly detected via Publicly Available Credentials)

- Keylogging Software **OC**
- Spyware Infected Downloads **OC**

Credential Stuffing

- Automated Attempts **I**
- Brute Force Attacks **I**

Unauthorized Account Creation (This will cross-link to the more detailed UAC tree)

- Create multiple accounts **I**
    - Account API
    - Stolen email addresses
- Potential unknown attack vectors via verbose error/API response **I**

Phishing Attacks

- Email Phishing
    - Impersonation of <company> Emails **OC**
    - Fake Subscription Renewal Alerts **OC**
- SMS Phishing (Smishing)
    - Fraudulent Security Alerts **OC**
    - Fake Promotions or Discounts **I**
- Social Media Phishing
    - Fake <company> Customer Support Accounts **I**
    - Phishing via Direct Messages **OC**

Exploiting Platform Vulnerabilities

Application and Website Exploits

- Application vulnerabilities (SQLI, XSS) **I**

- API Security Flaws **I**

Mobile App Vulnerabilities
- Exploiting Weaknesses in Mobile App Security **I**

Mobile App Exploits
- Reverse Engineering Mobile App for Vulnerabilities **I**
- Exploiting Sideloading on Android Devices **I**

Authentication Bypass

Password Reset and Account Recovery Exploits
- Intercepting Reset Emails or SMS **OC**
- Exploiting Account Recovery Questions **I**

Circumventing Two-Factor Authentication (when available)
- Phishing for 2FA Codes (N/A for now) **OC**

Insider/Other Threats

Compromised or Rogue Employees
- Misuse of Admin Privileges **I**
    - Accessing Sensitive Customer Data

Insider Threats Link to Insider Threat Attack Tree (IP)

Employee-Assisted Abuse
- Misuse of Access Privileges **I**
    - Accessing Sensitive Customer Data
- Collaboration with External Threat Actors **I**
- Internal Override of Trial Limits **IC**
- Employee-Created Ghost Accounts **IC**

Collusion with Insiders
- Obtaining Insider Information for Abuse **I**
- Assistance in Bypassing Account Restrictions **I**

Data Leakage
- Exfiltrating Customer Payment Data **I**
- Selling Sensitive Data to Third Parties **I**

Accidental
- Social Engineering Targeting CX agents **IC**
    - Phishing Attacks Against Staff
    - Pretexting to Gain Customer Information
- Overly permissive sharing **I**
- File Misconfigurations **I**