Use of AI and Machine Learning for Fraud Prevention

How to effectively mix AI and cyber intelligence for impactful identity fraud detection and prevention
“Retail loyalty programs, omnichannel shopping methods and customer identity manipulation have each experienced growth as a method for fraud attacks, increasing 89%, 23% and 30% respectively”

Cybercriminal beating identity detection measures throughout the ATO kill-chain

- Attackers methodologies used throughout ATO kill chain to avoid detection

**Credentials Compromise**
- Phishing / SMShing
- Malware
- Credentials Stuffing
- Social Engineering

**Login**
- Device Spoofing
- Virtual Machines
- Emulators
- Proxy//VPN
- Hosting services
- Overlay/RAT malware
- Social Engineering

**Account Recon**
- Proxy through user device
- Overlay/RAT malware
- Social Engineering

**Monetize**
- Proxy through user device
- Overlay/RAT malware

*Accelerated evolution using ML/AI to detect detection/protection patterns/gaps and evade them*
AI powered digital identity insight
Bot Detection - Using ML to distinguish machines from humans

- Cloud & Data Services solutions
- ISP
- Geo Location
- IP similarity
- Connection Details
- Server Characteristics
- Hardware and OS
- CPU
- Platform
- Screen Attributes
- Browser Characteristics
- Software
- Browser Attributes – Languages, Plugins, Properties
- Browser Version
- Multiple Accesses
- BOT Characteristics
- Behavior
- Key Strokes
- Mouse Movements
Phishing Detection
Machine learning classification based on website content scraping and analysis

HTML DOM Analysis
- number of links, images, JS Scripts, CSS, Iframes
- Internal/External to domain ratio for each element

Links Analysis
- Duplicated links, links referring to the same domain/page
- Links to social media services (Facebook, Twitter, ..)

Forms detection
- User input fields (text, email, password)
- Forms without SSL

Text Analysis
- Spelling Errors ratio
- Text/Code ratio

Image Analysis
- Text in image (OCR)
- Similarity with domain landing page

URL Analysis
- length, num of tokens
- TLD in URL
- Suspicious patterns
Many phishing attacks utilize vulnerabilities in benign web sites in order to inject their malicious phishing content.

A big difference in the screenshot between the landing page of a domain and the suspected URL is indicative of phishing.
AI based Logo detection (template matching, color histogram, location on page)
Behavioral Biometrics

- Keystrokes
- Time Spent on Page
- User Navigation Flow
- Mouse Movements
Real world use cases using AI powered digital identity trust
IBM Digital Trust Framework

**Assurance**
- Verify user claims of an unknown identity or attributes prior to establishing relationship
- Corroborate information with 3rd party intelligence sources

**Authentication**
- Validate users are who they are claiming to be based on previously established credentials
- Offer multiple different methods, including 3rd party
- Policy-based engine that binds together risk-assessment & authentication / verification
- Simplifies ongoing app development and provides visibility into outcomes

**Insights**
- Dynamic, multi-layered risk assessment across 5 context domains
- Output from this component drives follow-on actions (e.g., allow, block, authenticate)

**Orchestration**
- Discover
- Onboard
- Verify
- Logon
- Use
Digital customer identity top challenges

- Is it a human or a bot?
- Price and catalog scraping
- Automated reviews
- Automated purchasing (Black Friday, scalping)

- Is it the right human?
- Streamline buying and the checkout experience to increase conversion of true customers
- Avoid malicious activity by fraudsters
- Prevent Loyalty Program compromise (miles, points stealing)
Digital Trust top use cases

Establish trust during initial onboarding

Frictionless / Passwordless Login

Continuous trust validation
We need to change the way we think about our users.

Zero-trust does not facilitate great customers user-experience.

Most users should be given frictionless access to resources.

**Less than 0.05%** are suspected to be rogue and should trigger additional authentication measures.

Source: IBM Trusteer Research Case Study from Top 25 Global bank
The best security is the kind users don’t know is there

**Today’s Password-only Approaches**

- Hello...
- Who are you and what’s the password?
- It’s Jane and password is “Security”
- Wrong!
- Ugh! it’s “Security” with a “1” instead of the “i”
- You may enter

**Tomorrow’s Silent Security Approach**

- Hello...
- It’s Jane on her enrolled phone which is not jail broken or rooted, She is connecting from the usual region with no behavioral biometrics anomalies and her activity is in a low business-risk area.
- Come on in!
- Yippie!!!
Lets see this in action...
Shakedvax
MyPassword123!@#
More user AI identity insight yields better customer experiences

Silent Customer Experience

User Activity: User activity, timing, time on page, cross channel, user application behavior

Endpoint Environment: Geographic location, IP address/IP reputation of source, local time, etc.

Device Fingerprint: Screen depth/resolution, Fonts, OS, Browser/version, Browser plug-in, language, device model, etc.

User Identity Attributes: User Attributes, Groups, roles, credential attributes, organization

User AuthN: Username, Password, OTP, FIDO, Cert, QKB, reCaptcha

Endpoint Fraud Detection: Malware, Phishing, Remote Access Attack, Device Spoofing, and Anomalous Activity,

Behavioral Biometrics: Keystroke, mouse movement analysis, swiping patterns of access to apps, time of day
Digital Identity Trust Lifecycle Powered by AI and Machine Learning

Digital Identity Trust Platform

Trusteer Pinpoint Platform

ESTABLISH

Pinpoint Assure
Assess risk of new and unknown digital identities

SUSTAIN

Pinpoint Detect
Dynamic behavioral risk assessment of known digital identities

RECOVER

Pinpoint Verify
Increase trust level with flexible, strong authentication
Questions
Thank you

- Follow us on:
  - ibm.com/security
  - securityintelligence.com
  - ibm.com/security/community
  - xforce.ibmcloud.com
  - @ibmsecurity
  - youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.