The Trust Crisis: How Phishing Attacks Damage Your Brand and Bottom Line

Defending the Customer Journey Without Killing Conversions — A Guide for Banking Leaders

Yaamini Barathi Mohan

About Me

Yaamini Barathi Mohan

- Johns Hopkins University (JHU)
- Dell & RSA Security
- Researcher, Consultant
- Author
- Mentor
- WiCyS Austin - VP

Agenda

01

The Brand Cost of Phishing: Why Customers Blame You, Not Criminals

02

How Attackers Weaponize Familiar Banking UX (Login, OTP, Help Flows)

03

The CX-Security Seams: Where Your Teams Unintentionally Create Gaps

04

Confidence-Building Security: Reducing Takeovers Without Killing Conversion

05

Communicating Threats Clearly (Without Spooking Customers or Training Attackers)

06

Measuring True Cost: Reputational Damage + Brand Erosion

Case Study: How a Banking UX Pattern Became a Social Engineering Trap

01

Initial Contact

Phishing email mimics bank's legitimate communication style (fraud alert, account verification).

02

Familiar UX Trigger

Link directs to login page that mirrors the bank's exact design and error messaging.

03

OTP Interception

User enters one-time password, thinking they're completing legitimate verification.

04

Session Hijacking

Attacker gains access while customer believes they've successfully authenticated.

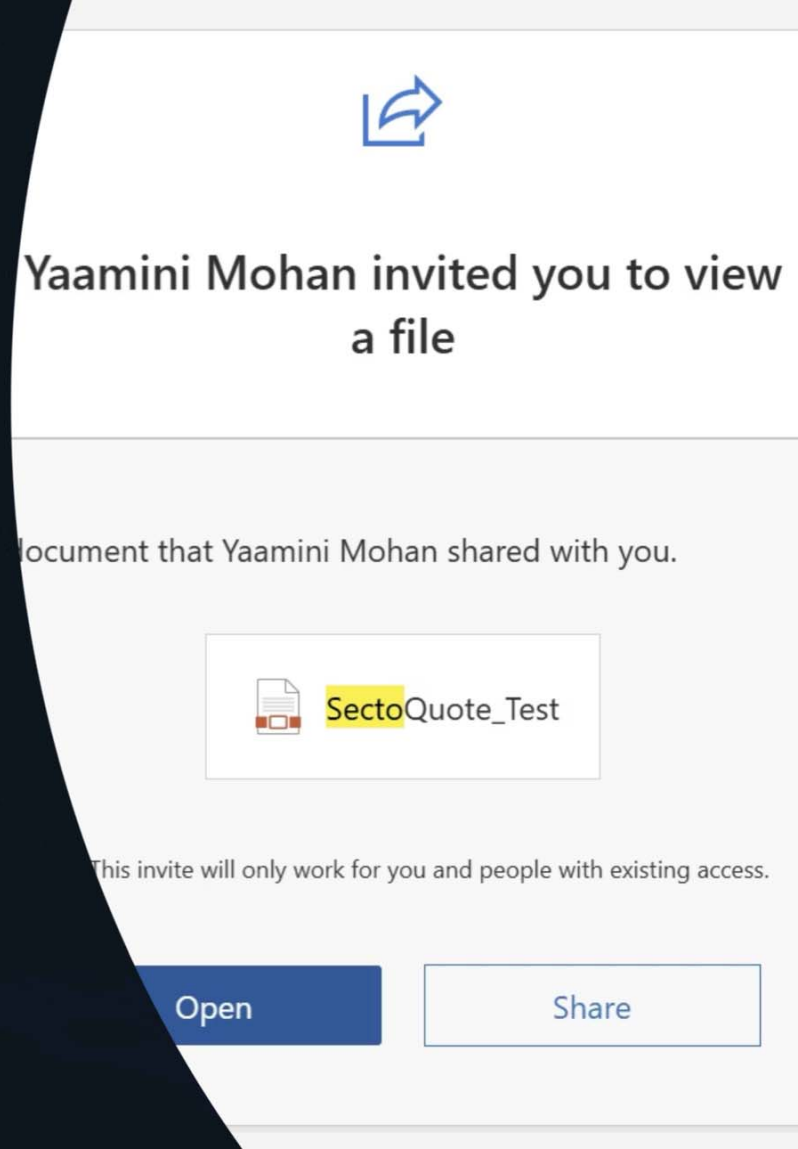
05

Account Takeover

Attacker transfers funds or changes account details before customer realizes compromise.

When a customer's account is compromised through a phishing attack, what's the biggest damage to your bank?

1. Direct financial loss from fraud
2. Customer churn and reputational damage
3. Regulatory fines and compliance costs
4. All of the above — and the reputational damage often exceeds the direct loss



The Growing Phishing Threat Landscape

500M

Phishing attacks annually

$4.5M

Average cost per breach

72%

Of customers who experience account takeover switch banks

91%

Involved in all cyberattacks

Why Banking Phishing Attacks Succeed: The CX-Security Gap

Attackers Exploit Familiar UX

Phishing pages mirror your login flows, error messages, and help prompts so closely that customers can't tell the difference. Attackers weaponize the very UX patterns you've optimized for conversion.

Organizational Silos Create Seams

CX, digital, fraud, and security teams operate independently. Attackers walk through the gaps between teams — using legitimate channels, trusted domains, and familiar patterns that no single team owns.

Modern Phishing Bypasses MFA: The Account Takeover Reality

- Attackers intercept OTP in real-time (AiTM attacks)
- Session hijacking gives them full account access
- MFA alone is not enough — you need confidence-building patterns

How Attackers Evade Your Defenses and Exploit Banking Channels

Conditional Loading

Links appear safe when scanned by security tools but redirect to phishing pages when customers click them minutes later.

Trusted Channels

LinkedIn, Slack, Discord, SMS — phishing isn't just email anymore. Attackers use channels your customers trust.

Legitimate Domain Abuse

Hijacking subdomains or abusing SharePoint, OneDrive, and Google Drive to host phishing pages on domains your security tools whitelist.

UX Mimicry

Replicating your exact login flows, error messages, and help prompts so customers willingly enter credentials and OTPs.

The Banking Reality: Where Your Customers Are Vulnerable

43%

Click Rate

Of customers who click phishing links despite security warnings

27%

Report Rate

Of phishing attempts actually reported to your security team

18

Average Days

Before account takeover is discovered (customer impact window)

How does your organization score? Most banks discover they're more vulnerable than they thought when tested with realistic phishing simulations tailored to banking UX patterns.

Confidence-Building Security: Protecting CX Without Killing Conversion

Don'ts

- Don't rely on email security alone — attackers use trusted channels
- Don't assume MFA is the silver bullet — use FIDO2, biometrics, and app-first verification
- Don't create friction that kills login/onboarding — customers will abandon you

Do's

- Do run simulations with realistic banking UX patterns (login, OTP, fraud alerts)
- Do align CX, digital, fraud, and security teams on shared threat models
- Do implement just-in-time warnings and safer deep links that build confidence without blocking conversions
- Do measure the true cost of account takeovers (reputational damage + churn, not just fraud loss)

Thank you

Yaamini Barathi Mohan