



Cybersecurity Awareness

Shane Harkins

Chief Information Officer, CISSP, CCSP

Staying Safe in the Age of AI

Disclaimer

The views, thoughts, and opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the official policy, position, or opinions of NDBT.

While every effort has been made to ensure accuracy and completeness, any errors or omissions are unintentional and the responsibility of the presenter.



Agenda

1 Since we last met

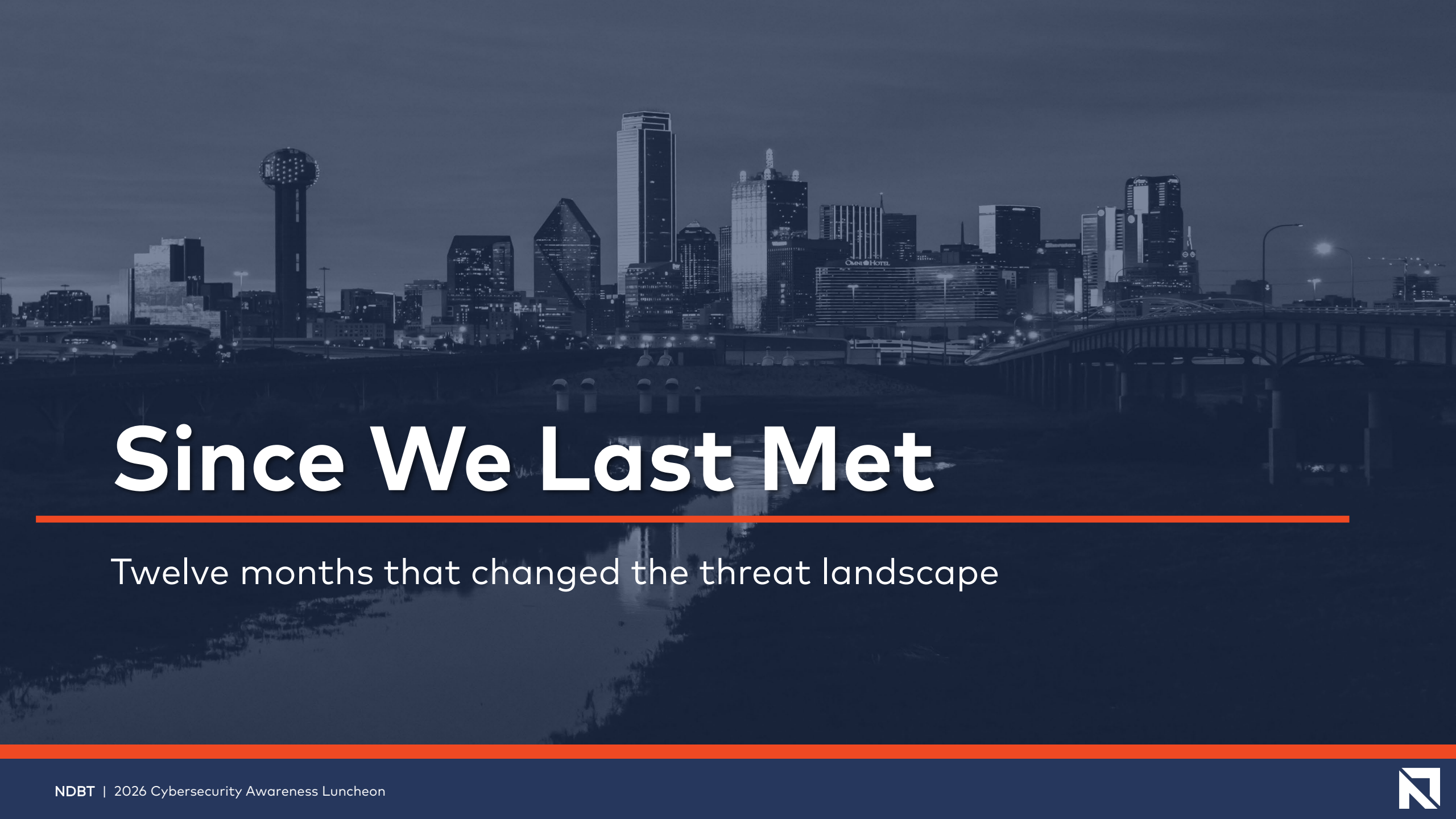
4 Artificial Intelligence

2 Phishing, new and old

5 Community scams and threats

3 Multi-Factor Authentication

6 How NDBT protects customers

A dark, monochromatic photograph of a city skyline at night, reflected in water. The skyline includes several prominent skyscrapers and a tall, thin tower with a spherical top. A bridge is visible in the foreground, spanning the water. The overall mood is somber and reflective.

Since We Last Met

Twelve months that changed the threat landscape

 SINCE WE LAST MET

The headline has shifted

31%

Vulnerability exploitation is now the #1 way in, passing stolen.

62%

of breaches still involve the human element. Attackers go through people because it works

AI

stopped being a helper and became an operator, running attacks end to end

AI is speeding up old tricks, not inventing new ones. The defenses that work today still work; we just have to move faster.

Source: Verizon 2026 Data Breach Investigations Report, Executive Summary



Phishing

Old technique, new delivery

What it is, and its many forms

Impersonating a trusted entity to trick people into revealing sensitive information.

Spear phishing

Targeted at a specific person or organization

Smishing

Phishing by SMS or text message

Vishing

Voice phishing over a phone call

Quishing

Phishing through a QR code (new, see next)

Two that are surging

Quishing (QR-code phishing)

~2 Million

unique malicious QR codes detected in the last nine months of 2025

- The malicious link is inside an image, so text-scanning email filters miss it.
- 1,642 brands impersonated in a single quarter.
- June 2025: NYC DOT warns of fake QR stickers on parking meters. Fall 2026: Sept 2026: 64 stickers later, an indictment.

Callback phishing (TOAD)

~10 Million

TOAD attempts per month

- No link, just a phone number and a reason to call. It sails past email filters.
- The victim calls a fake call center and is talked into handing over credentials.

Sources: APWG Phishing Activity Trends Reports, Q2 to Q4 2025 (data: Mimecast); Proofpoint; NYC DOT; Manhattan DA's Office

How to spot a real NDBT QR code

What if... that blank sticker was a stranger's code?

Here is what makes one of ours genuinely ours, so you can trust the codes we do send you.

A REAL NDBT CODE



Logo in the center, NDBT brand colors

HOW TO KNOW IT IS OURS

- It arrives in a context you expect: our statement, our letter, at our branches.
- When in doubt, do not scan. Browse to ndbt.com yourself or call us. (972) 716-7100

Banking & Finance sector specifically

Financial and Insurance (NAICS 52), how attackers get in

22%

Vulnerability exploitation

20%

Phishing

15%

Credential abuse

Even as the national headline moves to vulnerabilities, phishing and exploitation run nearly neck and neck for banks. And the human element is present in **65%** of financial-sector breaches, above the all-industry average. Our sector is still very much a phishing target.

Source: Verizon 2026 DBIR, Financial and Insurance (NAICS 52) industry breakdown



Multi-Factor Authentication

Not all MFA is created equal



What is phishing-resistant MFA?

Login methods that cannot be tricked into handing your credential to a fake site.

Each login is cryptographically tied to the real website address, so a lookalike page gets nothing.

HOW IT WORKS

Your device holds a secret key that never leaves it. When you log in, it proves who you are to the **real** site only. A fake site cannot receive that proof, and there is no code or password for anyone to steal, phish, or trick out of you.

WHAT COUNTS

- Passkeys
- Security keys
- Smart cards

GOOD, NOT BEST

Authenticator apps and push approvals beat a password alone. Texted codes are the weakest.

Why it matters: a regular code can be read to a scammer or typed into a fake page. A passkey cannot, because there is no code to give away. It is the only kind of MFA that stops a convincing fake site cold.



2025 MFA vs 2026 Phish-resistant MFA

Here is what phishing-resistant MFA does about each 2025 failure modes.

2025 failure mode	Why phishing-resistant MFA stops it
Adversary in the middle	Domain binding: the credential never works on the proxy site
SIM swapping	No phone number or SMS anywhere in the loop
MFA bombing / prompt fatigue	Nothing to approve, so there is no push to spam
Credential replay	Each login is cryptographically fresh and origin-bound

Source: CISA, Implementing Phishing-Resistant MFA fact sheet (2022)





Artificial Intelligence

From tool to operator



The moment AI crossed the line

AUG 2025

Vibe hacking

- One operator, one AI coding agent, at least 17 organizations extorted
- AI ran reconnaissance, credential harvesting, penetration, and wrote custom ransom notes.
- **Some demands topped \$500,000.**

NOV 2025

AI-orchestrated espionage

- A state-sponsored group manipulated the same class of tool against ~30 global targets.
- **Targets explicitly included financial institutions.**
- AI executed the attack, it did not merely advise.

The barrier to sophisticated attacks has dropped. One person can now do the work of an entire hacker team.

Source: Anthropic Threat Intelligence Report (Aug 2025); Anthropic, Disrupting AI-orchestrated espionage (Nov 2025)





The risk from inside

15% → 45%

of employees are now regular AI users on corporate devices, tripled in a year

67%

use non-corporate accounts to do it, outside any company control

Shadow AI. Your staff are likely pasting customer lists, payroll, and contracts into free AI tools on personal accounts. Set a simple rule: what can go in, and which tool to use.

Source: Verizon 2026 DBIR (Shadow AI / DLP findings)





Community Scams

Every one of them has an NDBT-published warning



The screenshot shows the top of the NDBT website. The header includes the NDBT logo, navigation links for PERSONAL, BUSINESS, TRUST | WEALTH, ABOUT US, CONTACT, and LEASING, a search icon, and a LOG IN button. Below the header is a large banner with a dark blue background on the left featuring a glowing shield with a padlock, and a red background on the right with white text. The text on the right reads: "Cybersecurity", "Learn About Ways to Better Protect Yourself and Your Assets", and a paragraph about the Risk Management Team. At the bottom of the banner is a red box with white text about an FCC public alert on bank impersonation scams.

 PERSONAL ▾ BUSINESS ▾ TRUST | WEALTH ▾ ABOUT US ▾ CONTACT ▾ LEASING ▾  [LOG IN](#)

Cybersecurity

Learn About Ways to Better Protect Yourself and Your Assets

NDBT's Risk Management Team works closely with all bank operations and often shares valuable tips and tools to our customers and clients to help ensure they are as protected from cyber threats as possible. Be aware and check back often!

The FCC (Federal Communications Commission) has issued a public alert warning consumers about bank impersonation scams that are currently on the rise. Please click this banner to read our recent blog highlighting these scams and offering tips to avoid becoming a victim.

Two that reach you at home

Screen Share, Beware

A text about "suspicious activity," a callback number, a move to FaceTime, then a request to share your screen while you log in.

Lesson: remote access is the new "give me your password." It defeats MFA. Never read an MFA code to anyone.

DocuSign impersonation

Real logo, an urgent "Review Document" button, and an invoice you never ordered with a number to "call and dispute the charge." The person who answers is the scammer.

Lesson: brand trust is the weapon, the same technique as the live demo. Talos lists DocuSign among the most impersonated brands..

Two more, and a pattern

Business Email Compromise (BEC)

A criminal poses as someone you already pay (a vendor, title company, or your boss) and emails "updated" wire or ACH instructions that route the money to them.

Lesson: never trust new payment instructions sent by email. Call the sender at a number you already have, not one in the message, before you send a dollar.

Bank impersonation

A call, text, or email claiming to be from NDBT about "suspicious activity," pushing you to verify a code, move money, or log in through their link.

Lesson: we will never call and ask for your online banking username or password, a code, your PIN, or your debit card number. Hang up and call the number on your card or our website.

Three of these four end in a phone call, and each one manufactures urgency. So, what happens when that urgent call comes from a voice you recognize?

How NDBT Protects Our Customers

What we do, and what you can turn on today

We guard our side. You can lock down yours.

What we do behind the scenes

- **Fraud monitoring:** we monitor for high-risk transactions and contact you when something looks off.
- **Trained staff:** our team is trained and phishing-tested, so scammers can't get to you through us.
- **Patched systems:** we find and fix weaknesses in our systems on a regular schedule.
- **Independent review:** outside auditors and bank regulators examine our controls regularly.

What you can turn on today

- **Alerts:** text or email notice of balances, transactions, and logins.
- **Card controls:** turn a card off and on, and set limits.
- **For businesses:** Positive Pay, dual approval on wires and ACH, and callback checks on any change to payment instructions.
- **Scam alerts:** current warnings at [NDBT.com/cybersecurity](https://www.ndbt.com/cybersecurity).

NDBT will never ask for your online banking username or password, a token code, your PIN, or your debit card number. We will never ask you to move money to “protect” it or to share your screen.

NDBT's Five

- 1** Slow down when you feel rushed. Urgency is the scam.
- 2** Hang up and call back on a number you trust. Never the one in the message.
- 3** Turn on the strongest MFA offered. And never read a code to anyone.
- 4** Don't scan a QR code you didn't go looking for. Type the address yourself.
- 5** Assume the voice and the face can be faked. Verify through a second channel. Agree on a family code word, and a verbal password for any payment request.

NDBT Risk Management is here to help. If something feels wrong, stop and call us: (972) 716-7100

“Trust, but Verify”



DO NOT Trust, Verify!

References (1 of 2)

#	Source	Publisher	Supports
1	2026 Data Breach Investigations Report	Verizon	Vuln, Phishing, AI
2	Threat Intelligence Report (vibe hacking)	Anthropic	AI
3	Disrupting AI-orchestrated espionage	Anthropic	AI, Since We Last Met
4	ARTEX: AI attacks on Korean banks	CrowdStrike	AI
5	Parking Meter Scam Advisory	NYC DOT	Phishing (quishing)
6	PDFs as phishing delivery / TOAD	Cisco Talos	Phishing (callback)
7	State of the Phish	Proofpoint	Phishing (callback)
8	2025 Internet Crime Report	FBI IC3	Community Scams (BEC)

Government, law enforcement, standards bodies, established industry research, and NDBT's own published material.

References (2 of 2)

#	Source	Publisher	Supports
9	Implementing Phishing-Resistant MFA	CISA	MFA
10	SP 800-63-4 Digital Identity Guidelines	NIST	MFA
11	Federal Zero Trust Strategy (M-22-09)	US OMB	MFA
12	Passkeys / FIDO2 guidance	FIDO Alliance	MFA
13	Cybersecurity scam alerts	NDBT Risk Mgmt	Community Scams
14	Spot and Stop Bank Impersonation	NDBT	Community Scams
15	Bank impersonation scam guidance	US FTC / FDIC	Community Scams
16	Phishing Activity Trends Reports, Q2–Q4 2025	APWG (data: Mimecast)	Phishing (quishing)
17	Parking-meter QR sticker arrest and charges	Manhattan DA's Office	Phishing (quishing)
18	2025 Internet Crime Report	FBI IC3	Community Scams (BEC)

Government, law enforcement, standards bodies, established industry research, and NDBT's own published material.