PROTECT YOUR ACCOUNTS

Corporate Customer Account Takeover & Information Security

Customer-ready awareness presentation | 2026

CATO

Prevention + readiness

Security awareness training goals

Use this deck to explain CATO risk, attack patterns, defenses and response actions.

Define CATO

Explain how account takeover can lead to fraudulent online banking activity.

Recognize threats

Review malware, viruses, spyware, scareware, phishing, hoaxes and email-based risk.

Protect the business

Translate safeguards into practical user and control behaviors.

Respond quickly

Clarify customer incident response planning and immediate actions.

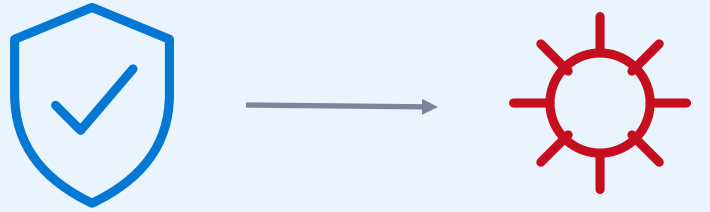
What is Corporate Account Takeover?

CATO is a credential theft and fraudulent payment risk for business online banking.

CATO in plain language

Cyber thieves steal employee passwords and other valid credentials.
They gain control of business bank accounts.
Fraudulent wire, ACH, online bill pay and payroll payments can be initiated.

Key message: business safeguards and payment controls are part of fraud prevention.



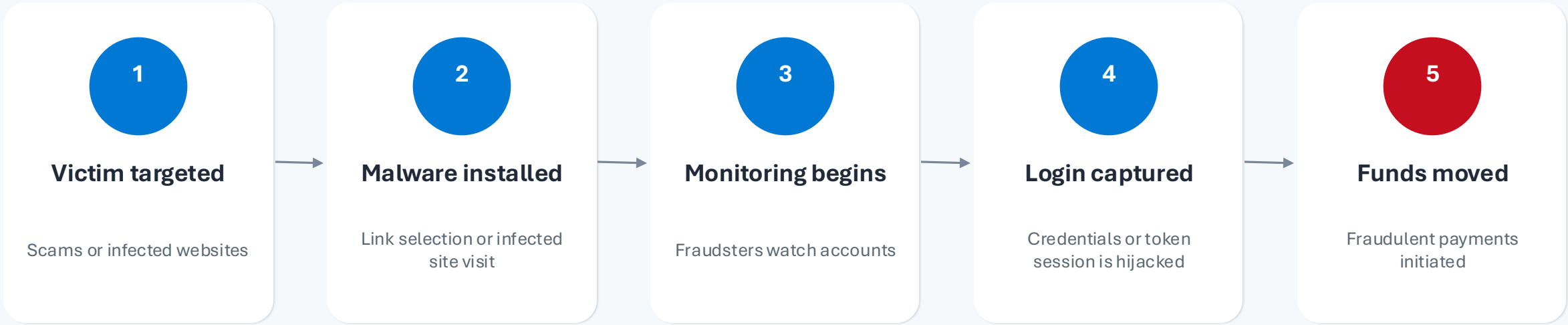
Credentials **Account access**

Fraudulent transactions

Wire | ACH | Bill Pay | Payroll

How does a CATO attack work?

A typical pattern starts with scams or infected sites and ends with credential capture or session hijacking.



Presenter tip: emphasize that controls and training can interrupt this chain at multiple points.

Threat landscape: what customers should recognize

Customer awareness should cover malware categories and social engineering methods.

Malware

Software designed to infiltrate a system without informed consent.

Viruses

Programs that can copy themselves and infect computers.

Spyware

Hidden software that collects information about users.

Scareware

Fraudulent software that misleads users into paying for fake malware removal.

Phishing

Fraudulent attempts to acquire sensitive information by masquerading as trustworthy.

Hoaxes

Tricks or scams that may prompt harmful actions or disclosure.

Where do threats come from?

The references highlight web, email, peer-to-peer downloads and ads as major paths.

Common entry points

Malicious websites, including social networking sites
Email
P2P downloads and file-sharing sites
Ads from popular websites

Email is fast, scalable and therefore heavily abused.

Questions for customer teams

1. Can employees spot suspicious attachments?

2. Are payment users trained to pause on unusual prompts?

3. Are pop-ups and browser add-ons controlled?

4. Do users know how to report suspicious activity?

What can businesses do to protect accounts?

The training material emphasizes layered controls across people, devices, access and transactions.

People

Train employees
Be alert for suspicious email
Know reporting paths

Devices

Maintain antivirus, antispyware and firewall tools
Apply security updates
Use spam filters and block pop-ups

Access

Limit administrative rights
Require software approval
Avoid public internet access points

Transactions

Reconcile accounts daily
Use dual control from separate devices
Assess online-payment risk and insurance coverage

Layered security works best when customer teams know both preventive controls and escalation steps.

Incident response: be ready before a suspicious event

Customer response planning should include contacts, transaction controls and recovery support.

Plan components

Direct contact numbers for key Bank personnel
Steps to limit unauthorized transactions
Information needed to support funds recovery
Insurance carrier contact procedures
Forensic specialist or law enforcement coordination when appropriate

Immediate actions to consider

Change passwords
Disconnect computers used for online banking
Request temporary holds until out-of-band confirmations can be made

Report suspicious activity to the company and bank. Contact the Bank if a fraudulent transaction is suspected or a suspicious bank-themed email requests personal or company information.

304 534 7200

Mobile banking security checklist

Use these customer-facing tips to reduce risk when accessing accounts from mobile devices.

Device basics

Do not share or save PINs, passwords or security questions on the phone
Password-protect the device
Report a stolen smartphone to the wireless provider

Browser use

Log out and close the browser
Use secure, encrypted websites
Avoid public Wi-Fi when possible
Do not follow links from emails that appear to be from the bank

App use

Log out of the application when not using it
Add mobile security software to the device, if possible
Monitor records and accounts regularly

Close: train, verify, report and respond quickly.