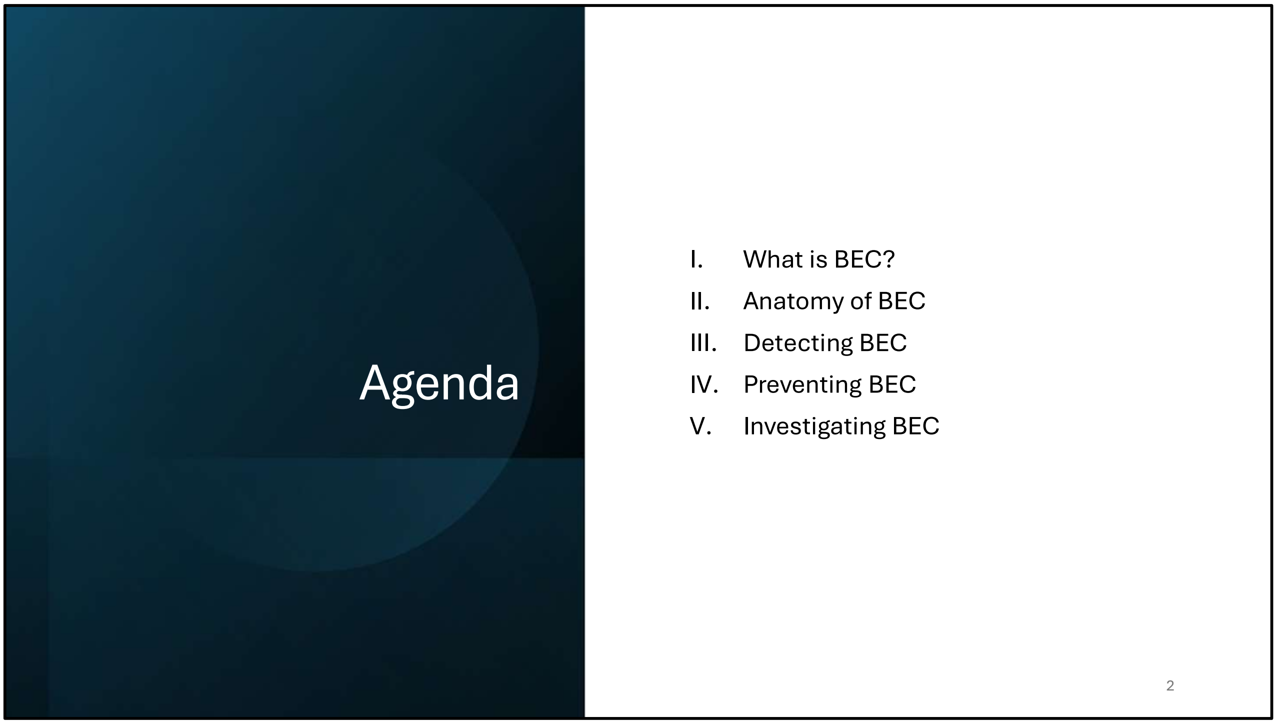
Business Email Compromise (BEC) Investigations

MassCyberCenter
at the MassTech Collaborative

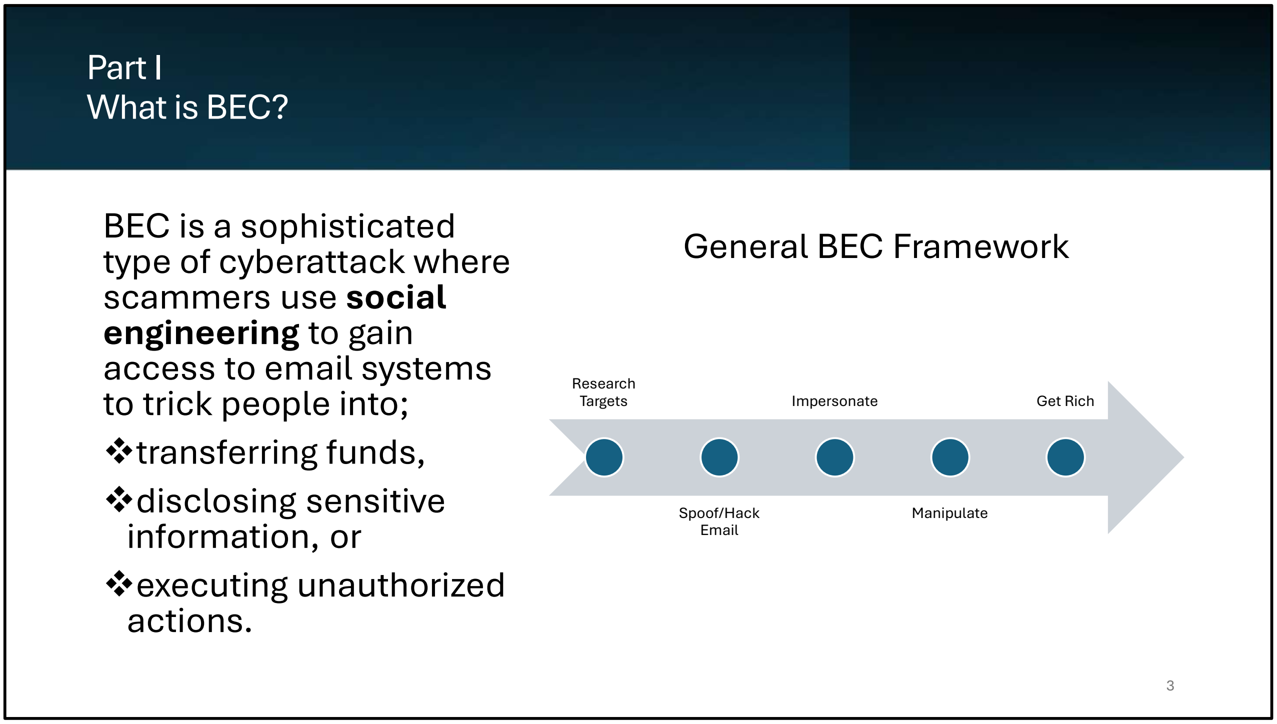
John Petrozzelli, Director

September 2024



Agenda

I. What is BEC?
II. Anatomy of BEC
III. Detecting BEC
IV. Preventing BEC
V. Investigating BEC



Part I
What is BEC?

BEC is a sophisticated type of cyberattack where scammers use **social engineering** to gain access to email systems to trick people into;

❖transferring funds,

❖disclosing sensitive information, or

❖executing unauthorized actions.

General BEC Framework

Research Targets

Spoof/Hack Email

Impersonate

Manipulate

Get Rich

BEC is a sophisticated type of cyberattack where scammers use **social engineering** to gain access to email systems to trick people into;
❖transferring funds,
❖disclosing sensitive information, or
❖executing unauthorized actions.

Social engineering is when hackers use psychological manipulation techniques to trick users into making security mistakes or giving away sensitive information.

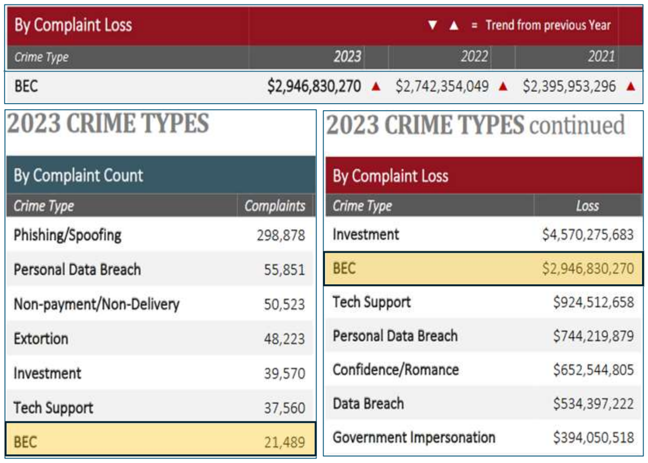
There are a variety of different ways hackers implement BEC attacks. However, regardless of the specific type of BEC, they all share a general framework;

1. Research Targets
2. Spoof or Hack Email
3. Impersonate
4. Manipulate
5. Get Rich

How Serious is BEC?

- $ Approx $3Billion in losses
- # 21,489 cases reported
- $137,000 average loss
- Low technical skills

FBI Cyber Crimes Report 2023



By Complaint Loss ▼ ▲ = Trend from previous Year

Crime Type	2023	2022	2021
BEC	$2,946,830,270 ▲	$2,742,354,049 ▲	$2,395,953,296 ▲

2023 CRIME TYPES

By Complaint Count

Crime Type	Complaints
Phishing/Spoofing	298,878
Personal Data Breach	55,851
Non-payment/Non-Delivery	50,523
Extortion	48,223
Investment	39,570
Tech Support	37,560
BEC	21,489

2023 CRIME TYPES continued

By Complaint Loss

Crime Type	Loss
Investment	$4,570,275,683
BEC	$2,946,830,270
Tech Support	$924,512,658
Personal Data Breach	$744,219,879
Confidence/Romance	$652,544,805
Data Breach	$534,397,222
Government Impersonation	$394,050,518

https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

According to the FBI 2023 Cyber Crimes Report, there were 21,489 reported cases of BEC last year totaling almost $3 billion in losses, with an average of $137,000 per case. I wish I ran a company that grossed $3 billion. It's also safe to assume these estimates are low, as organizations are often hesitant to report such activity. In the world of cybercrime, BEC attacks are very appealing to attackers because a little effort can yield significant rewards. Further, unlike a lot of other cybercrimes that require advanced technical expertise or expensive equipment, BEC attacks can be successful with just one well-planned email.

How are Companies at Risk?

- Procurement Fraud
- Vendor Payments
- Payroll Diversions
- Data Breaches
- Grant & Aid Fund Misappropriation

5

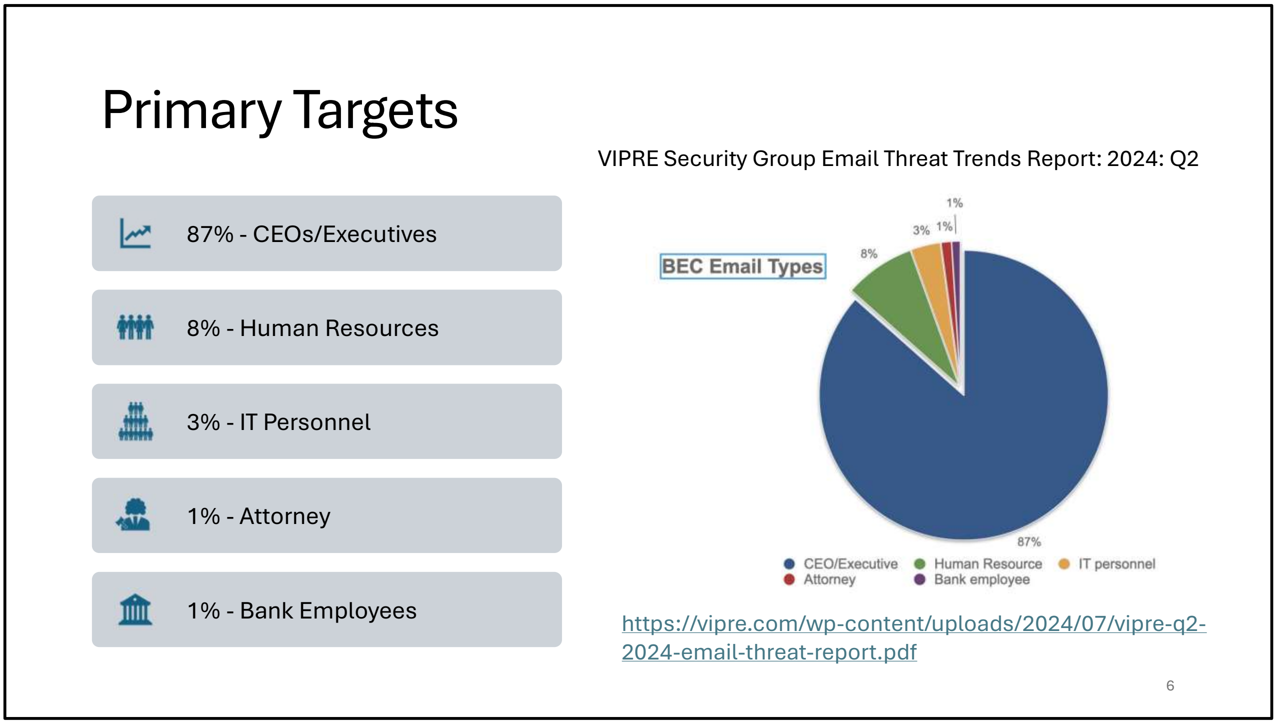
There are many different types of business email compromise. Some of the most common BEC attacks against municipalities include, but are not limited to;

Procurement Fraud & Vendor Payments: Municipalities handle substantial payments to vendors, contractors, and service providers. Attackers can exploit these transactions by sending fraudulent emails that redirect payments to accounts controlled by cybercriminals. For example, a local government may receive a spoofed email from a legitimate vendor requesting a change in banking details for an upcoming payment. If unverified, the funds could be transferred to the attacker's account.

Payroll Diversion: Payroll departments are vulnerable to BEC attacks where attackers request changes to direct deposit details. This can lead to employees' salaries being diverted to fraudulent accounts. For example, a municipal employee may receive a seemingly legitimate email requesting an urgent update to direct deposit information. Without proper verification, the payroll funds could be stolen.

Data Breaches: Local and state governments manage sensitive data, including personal information of residents, employee records, and law enforcement details. BEC attacks can be used to steal this data, which can then be sold on the dark web or used for further attacks. For example, an attacker may impersonate an IT administrator to gain access to government databases, leading to the exposure of sensitive citizen data.

Misappropriation: Governments often manage large sums of money from federal aid or grants, particularly during crises like natural disasters. Attackers can target these funds through BEC schemes, redirecting them to fraudulent accounts. For example, during a crisis, attackers may impersonate federal agencies or NGOs to misdirect relief funds.



Primary Targets

- 87% - CEOs/Executives
- 8% - Human Resources
- 3% - IT Personnel
- 1% - Attorney
- 1% - Bank Employees

VIPRE Security Group Email Threat Trends Report: 2024: Q2

https://vipre.com/wp-content/uploads/2024/07/vipre-q2-2024-email-threat-report.pdf

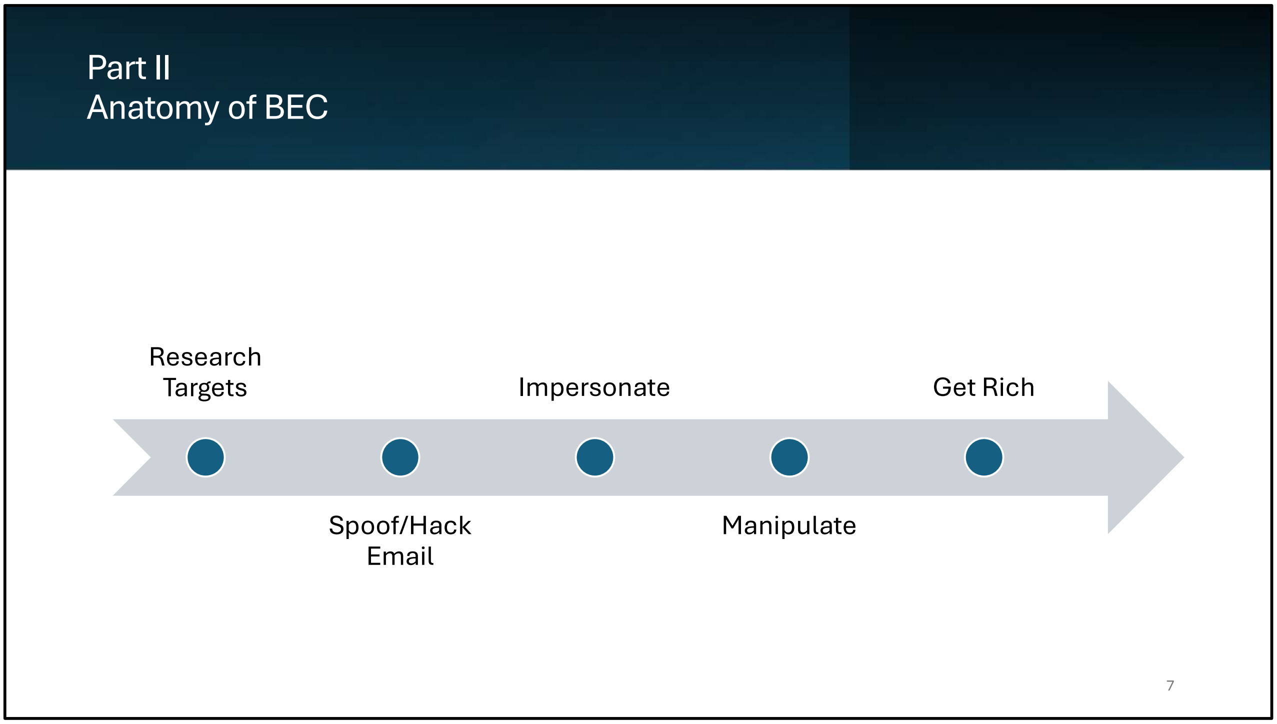
6

In order to carry out these attacks, hackers are generally looking for CEOs, CFOs, COOs, Legal Counsel, the big fish who have the authority to make things happen. Ultimately, hackers want to impersonate people with the power and authority to manipulate lower-level employees. However BEC can happen to anyone.

Sometimes hackers are looking for employees to impersonate to redirect paychecks to the hacker's bank account.

Other times, the hacker wants to impersonate a vendor to redirect payments to the hacker's bank account.

There are a wide variety of ways the hackers can successfully implement a BEC attack.



Part II
Anatomy of BEC

Research Targets

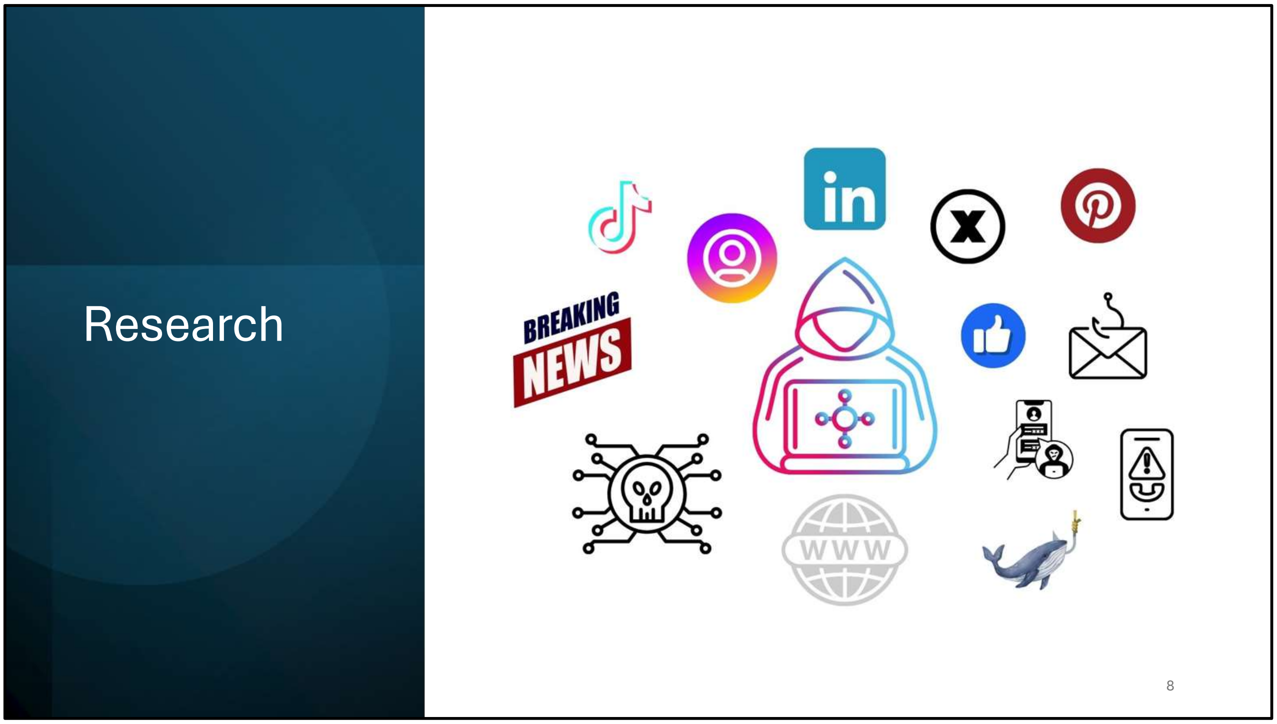
Spoof/Hack Email

Impersonate

Manipulate

Get Rich

Now that we know what BEC is, we are going to look at the steps hackers take to carry out these attacks.



Research

The first step to a successful BEC attack is research and information gathering. Hackers engaged in BEC attacks do their homework. Specifically, they are looking for names, job titles, email address structures, domain names, vendors, customers, etc. They want to understand how money and information move in and out of an organization. They are also looking for additional personal information to add context to their communications, and today this type of information can be found easily in a variety of places;

Linked In,
Online Directories
Phishing, Smishing, Vishing, Whaling – we'll get into more detail on these terms in the next slide.
Dark Web – it's a real thing
News Articles
And of course, Social Media

Based on what they learn, they will design ways to collect more information from you.

Phishing

Phishing

Smishing

Vishing

Whaling

BEC hackers will send out;

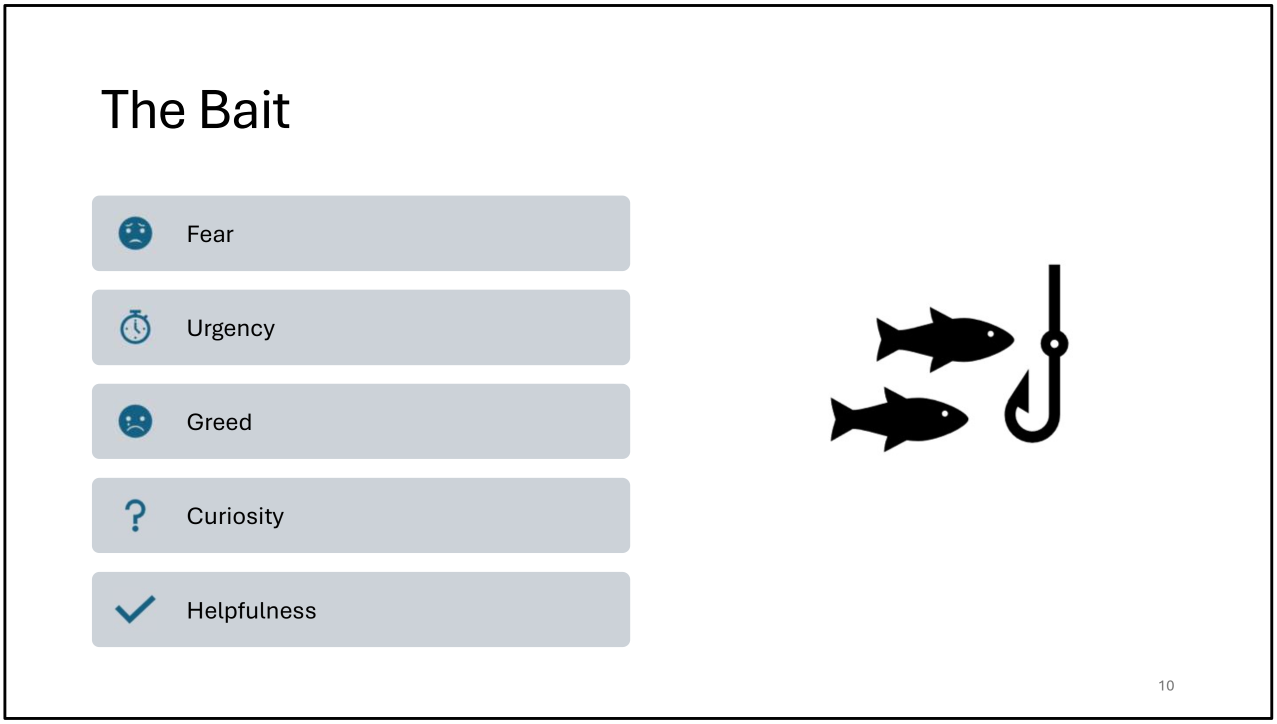
Phishing is when attackers send out email attachments that can contain malware, such as viruses, spyware, adware, worms, botnets. This malware can be used to steal confidential data, gain access to networks, or carry out other malicious actions. Emails may also contain links to spoofed or dangerous websites designed to collect your data.

Smishing is a type of phishing attack that uses text messages to deliver a fraudulent link or attachment. Smishing is especially threatening because people are more likely to trust text messages than emails.

Vishing is when hackers call targets to gather more data via phone call. Usually, the phone call is followed up with an email or text to lure victims into clicking on malicious links or attachments.

Whaling is simply a phishing attack targeted directly at executives.

Their ultimate goal is to gain access to your accounts. However, even if they fall short of this, they can still implement a successful BEC attack.



The Bait

- Fear
- Urgency
- Greed
- Curiosity
- Helpfulness

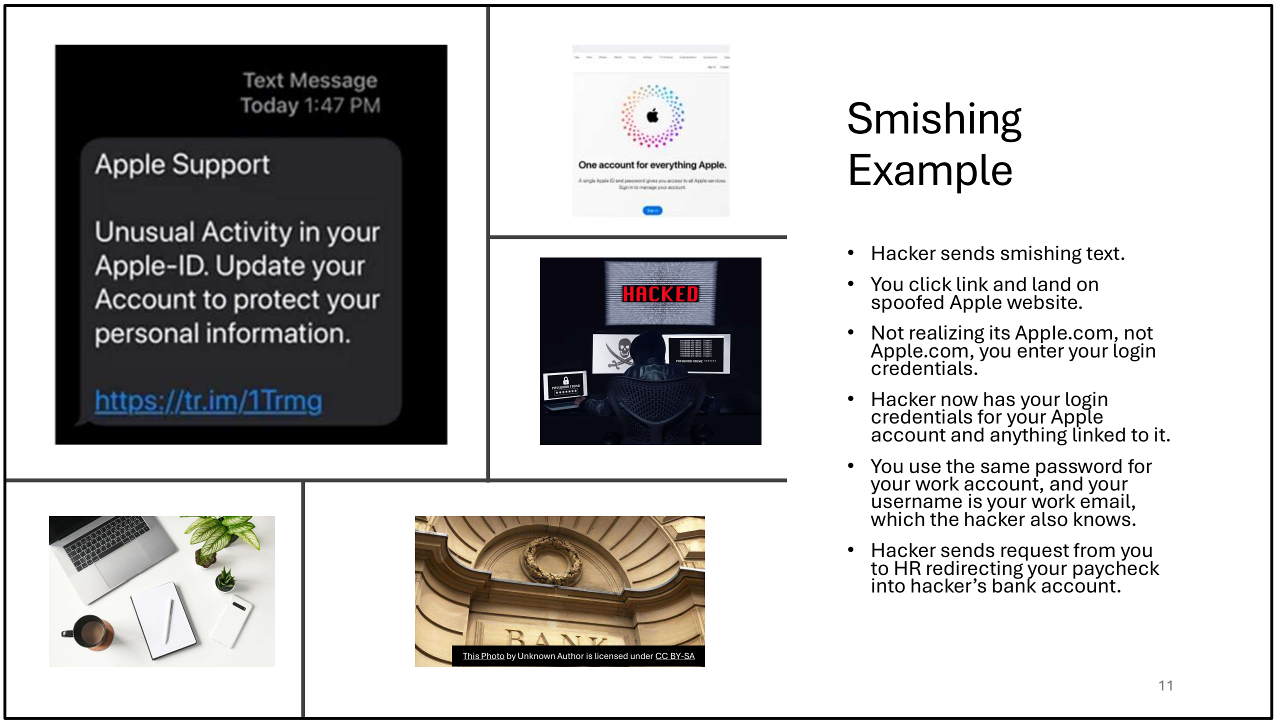
10

https://www.tripwire.com/state-of-security/beyond-firewall-how-social-engineers-use-psychology-compromise-organizational

These phishing attempts will be designed to manufacture certain emotions that make you easier to manipulate.

Fear – Fear is among the strongest emotions to raise anxiety. This becomes a powerful manipulator, and the attacks that use fear are more likely to be successful. An urgent bank account compromise notification is a common instance that generates fear in someone, and may cause them to click an infected link to take action to correct the problem.
Urgency – Fake security alerts such as urgent bank notifications, virus notifications, account login, and password change notifications will generate a feeling of urgency to make quick decisions without a second thought.
Greed – Greed is an intense and selfish desire to acquire something. A phishing email offering free subscription services, discounts, and rewards would lure many unknowingly to harmful actions.
Curiosity – The desire and interest to know something is sometimes a vulnerability for social engineers. Messages involving popular or sensitive topics, or links to risqué photos may quickly gain attention from someone.

Helpfulness – People tend to be more helpful towards others when they are in need, this quality is exploited in ways such as asking for fake donations, assistance, and information.



Text Message
Today 1:47 PM

Apple Support

Unusual Activity in your Apple-ID. Update your Account to protect your personal information.

https://tr.im/1Trmg

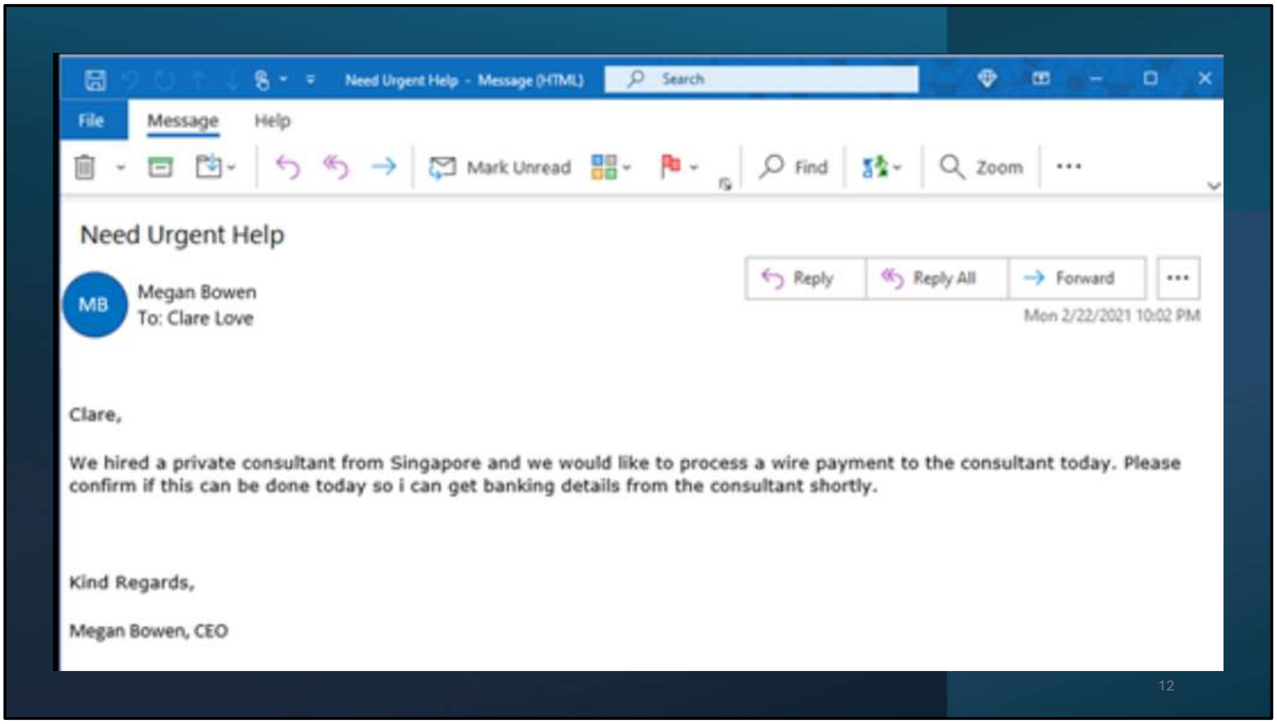
This Photo by Unknown Author is licensed under CC BY-SA

Smishing Example

- Hacker sends smishing text.
- You click link and land on spoofed Apple website.
- Not realizing its Apple.com, not Apple.com, you enter your login credentials.
- Hacker now has your login credentials for your Apple account and anything linked to it.
- You use the same password for your work account, and your username is your work email, which the hacker also knows.
- Hacker sends request from you to HR redirecting your paycheck into hacker’s bank account.

11

Victim receives a **smishing** text message that appears to be a legitimate Apple support text message.
Victim clicks the link and is directed to a fake Apple website. Appl(capital i)e.com
Victim logs in, and now the hacker has captured the victim’s Apple account login credentials.
Unfortunately, the victim’s work account is also connected to Apple ID.
Now the hacker impersonates the victim and asks HR to update banking information.
On payday, the victim’s paycheck is deposited into the hacker’s account.



Need Urgent Help

Megan Bowen
To: Clare Love

Mon 2/22/2021 10:02 PM

Clare,

We hired a private consultant from Singapore and we would like to process a wire payment to the consultant today. Please confirm if this can be done today so i can get banking details from the consultant shortly.

Kind Regards,

Megan Bowen, CEO

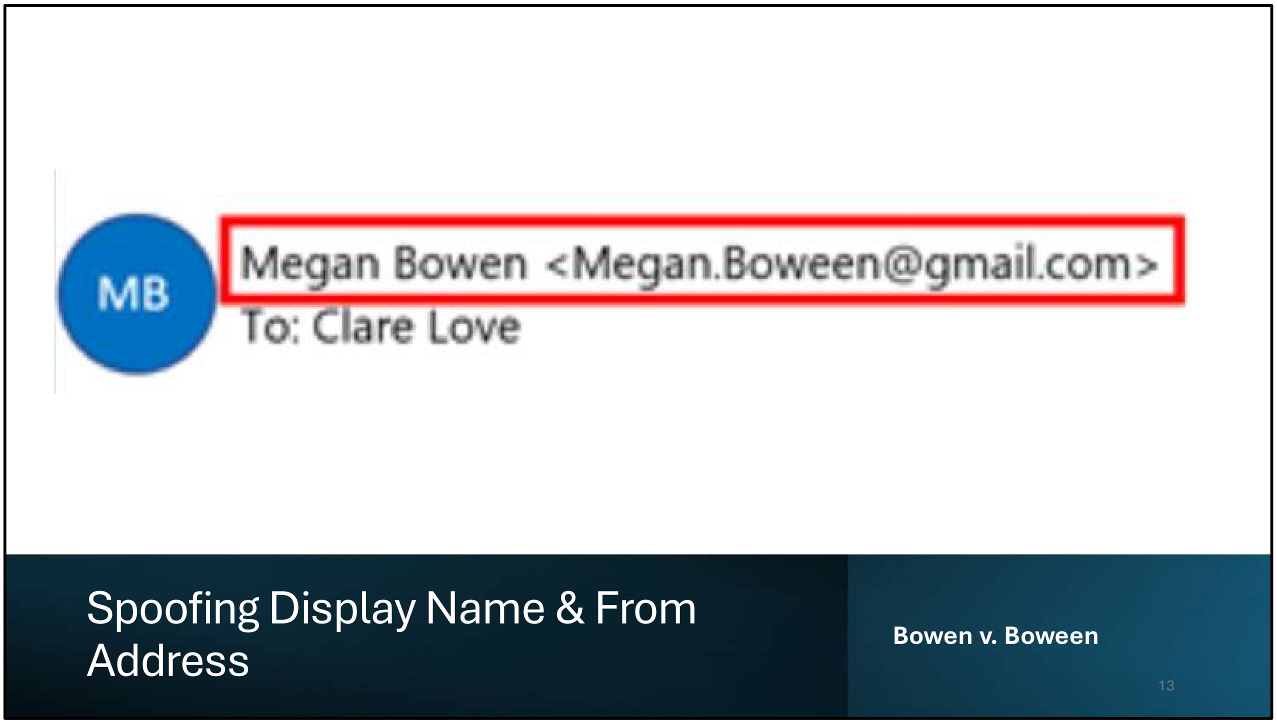
https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900

Here we have an example email. It says Need Urgent Help, there's your first clue.

It also says that they hired a private consultant from Singapore, for most municipal employees, that would be considered unusual.

It goes on to say that the payment needs to be processed today, creating a sense of urgency.

Lastly, it appears to be from the CEO, so the hacker is using power and influence, maybe even fear, to manipulate this employee into compliance.



Megan Bowen <Megan.Boween@gmail.com>
To: Clare Love

Spoofing Display Name & From Address

Bowen v. Boween

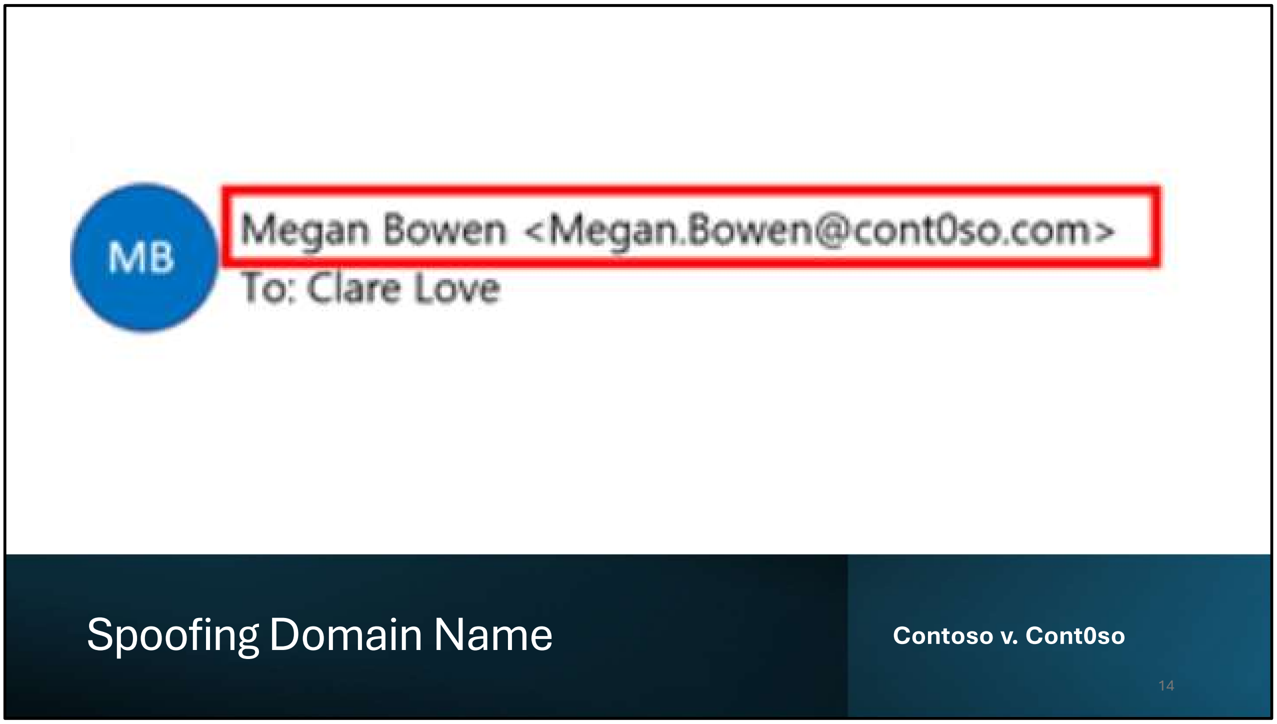
13

https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900

However, if you take a close look at the email, you will notice that although the display name appears to be correct, the last name in the From Address is spelled incorrectly. Not to mention the gmail address.

A spoofed email is an email that is designed to look like it came from a legitimate person. However, if you look closely at the display name, and sender email, or click return to and inspect the return to email, you will see that there is a subtle difference somewhere that indicates the email is fake. This is surprisingly simple to do.

With a spoofed display name, it looks like the email is coming from a trusted source. Most people don't even verify the from email. A close look here would alert an end user to the possibility that something is off. The challenge with BEC is that there is no technical control to prevent this, only effective awareness and training.



Megan Bowen <Megan.Bowen@cont0so.com>
To: Clare Love

Spoofing Domain Name

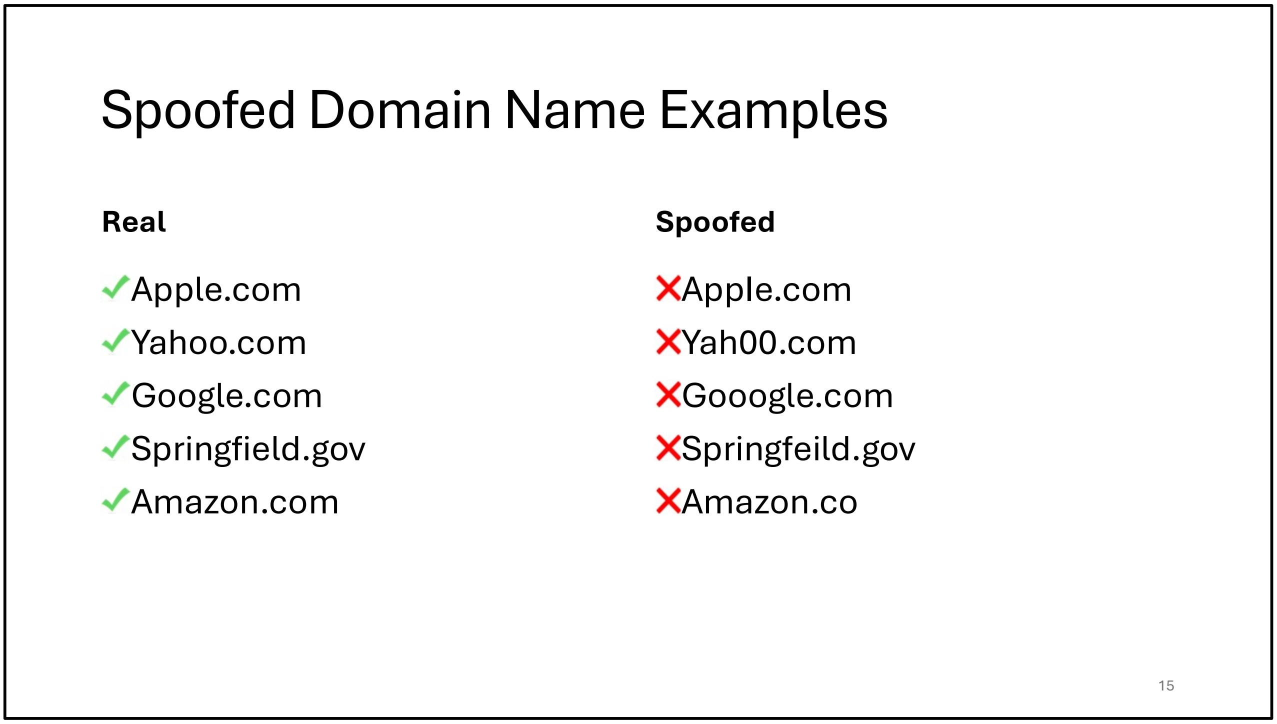
Contoso v. Cont0so

14

https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900

Sometimes hackers will take the extra step of spoofing the domain name. Here the hacker registered a domain name similar to the company name, Contoso, but switched out an o for a zero.

Technical controls may or may not catch this, only people who know what to look for.



Spoofed Domain Name Examples

Real	**Spoofed**
✓Apple.com	✗Apple.com
✓Yahoo.com	✗Yah00.com
✓Google.com	✗Gooogle.com
✓Springfield.gov	✗Springfeild.gov
✓Amazon.com	✗Amazon.co

15

There are multiple ways that hacks can spoof domain names. A few examples include;

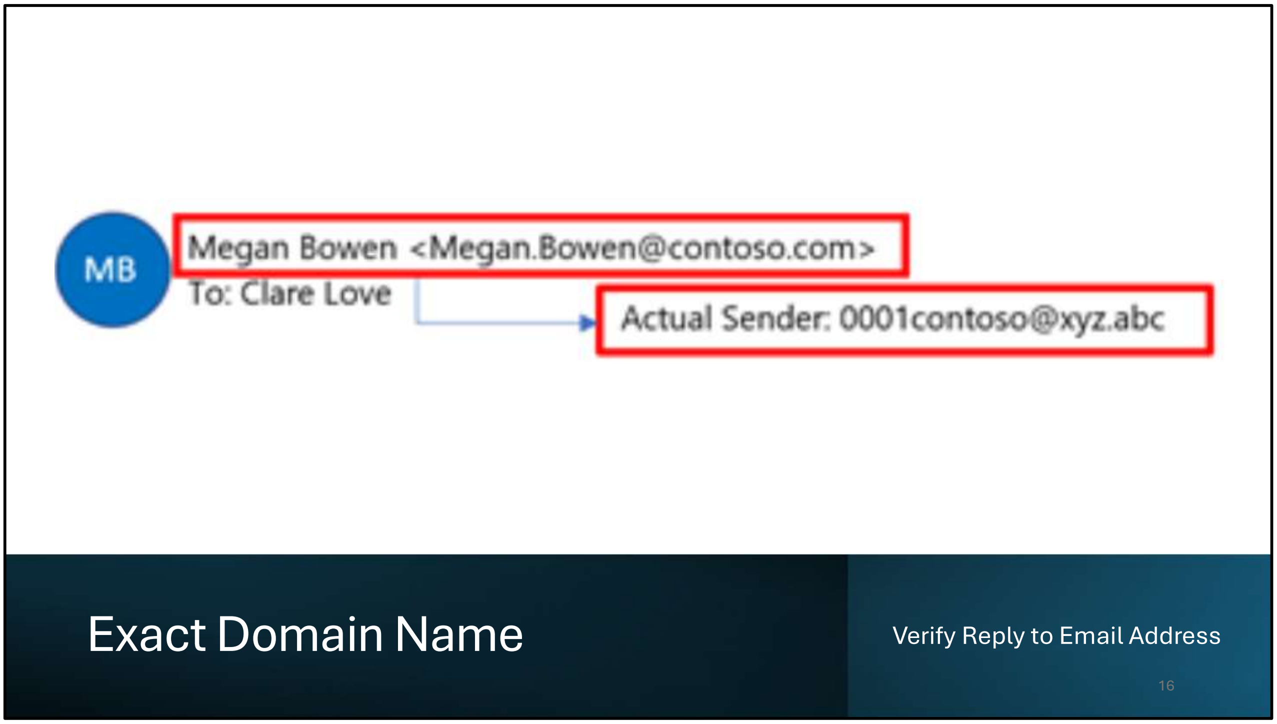
1. Using letters that look like other letters like the spoofed website uses a capital i instead of a lowercase l.

2. Replacing letters with numbers like the spoofed Yah00.com that replaced the o’s with zeros.

3. Adding/Removing Letters – Gooogle.com

4. Transposing Letters – the spoofed Springfield.gov replaced the p with a q and transposed the e and the i. PowerPoint’s autocorrect didn’t even flag it.

5. Registering identical domains under different top-level domains like the spoofed Amazon.co



Megan Bowen <Megan.Bowen@contoso.com>
To: Clare Love

Actual Sender: 0001contoso@xyz.abc

Exact Domain Name

Verify Reply to Email Address

16

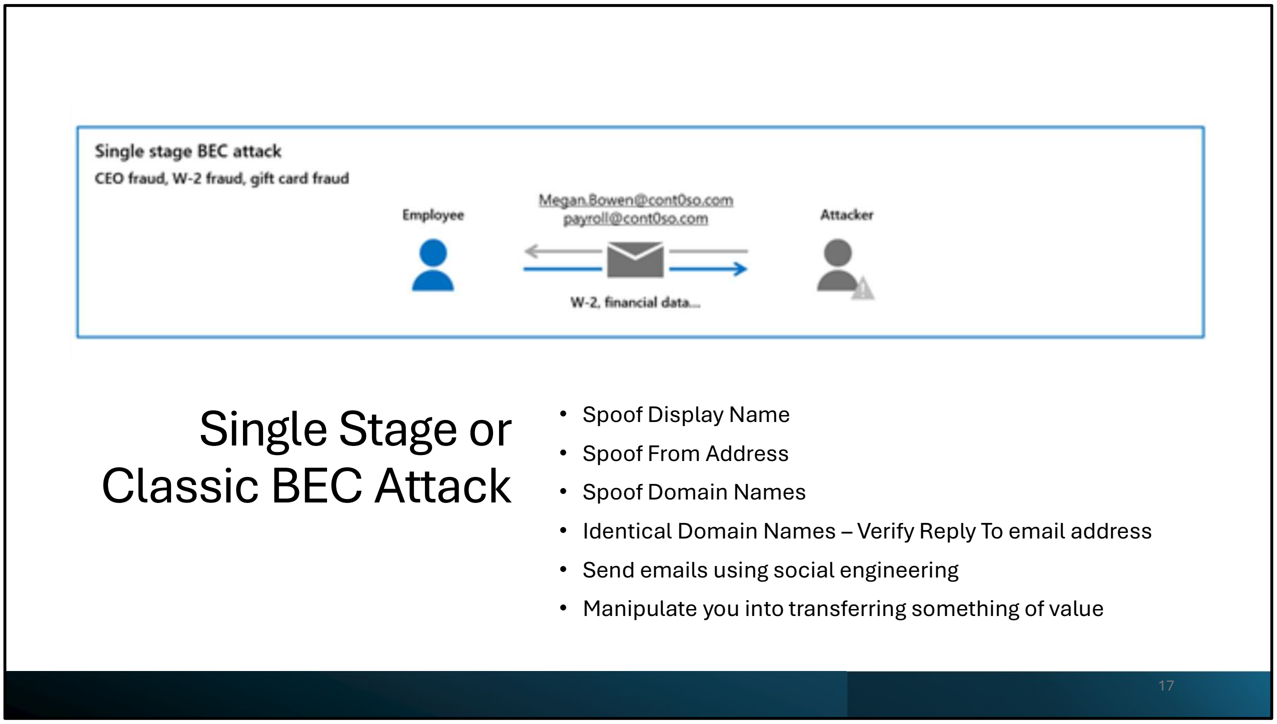
https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900

Hackers can even make the From Address Domain name identical, but have the Reply-To Address be something completely different.

It is possible to set up technical controls by implementing email authentication standards;

Sender Policy Framework (SPF)
DomainKeys Identified Mail (DKIM)
Domain-based Message Authentication Reporting and Conformance (DMARC)

However, these are not foolproof, if the domain does not have these set up, the domain can be spoofed. Having trained personnel is still your best defense.



Single stage BEC attack

CEO fraud, W-2 fraud, gift card fraud

Employee
Megan.Bowen@cont0so.com
payroll@cont0so.com
Attacker
W-2, financial data...

Single Stage or Classic BEC Attack

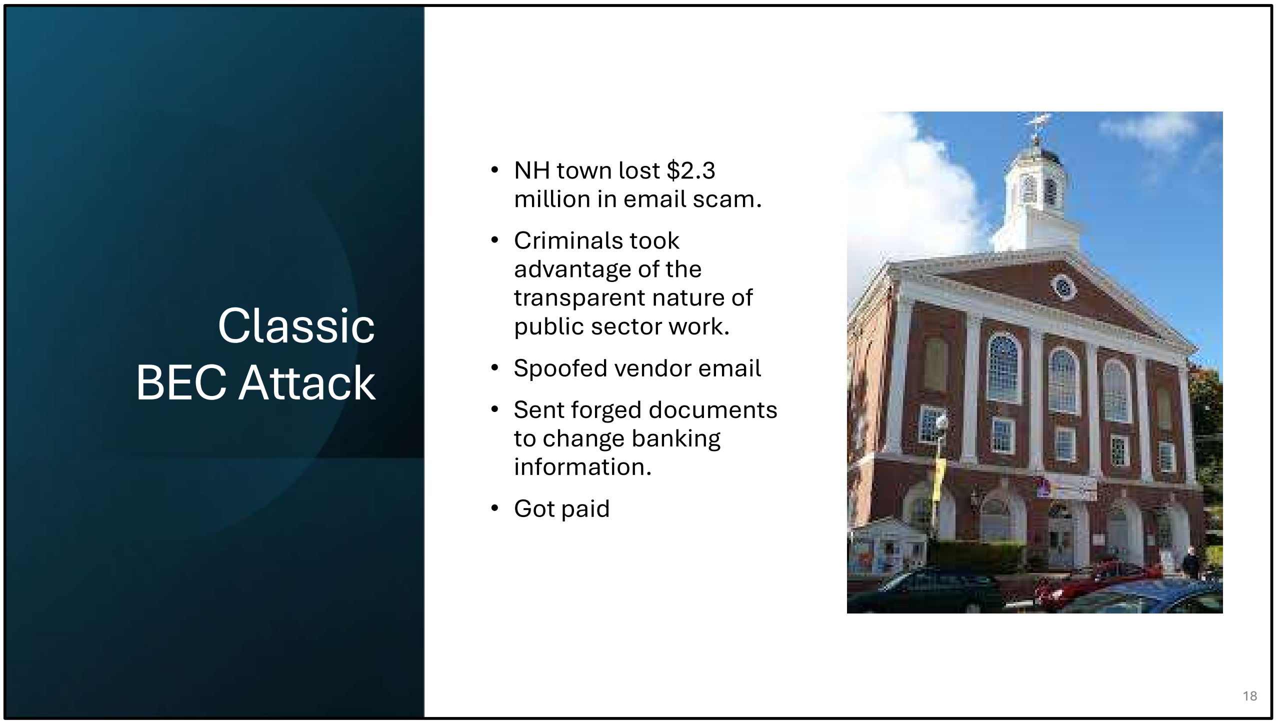
- Spoof Display Name
- Spoof From Address
- Spoof Domain Names
- Identical Domain Names – Verify Reply To email address
- Send emails using social engineering
- Manipulate you into transferring something of value

https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-one/ba-p/2159900

Using one or more of the strategies above, hackers can easily implement a classic or single-step BEC attack, even without full hacking and accessing your email.

In a single-stage attack, the hacker spoofs emails and domain names to impersonate executives, business partners, human resources, finance departments, and so on, to manipulate them into processing things like redirected payments into the hacker's bank accounts or sharing valuable confidential information, like w2s for all staff.

As mentioned above, everyone needs to understand how hackers can spoof **display names**, **from addresses**, and **domain names,** and remember to always check the Reply To address because technical controls are often of limited use, people are the best defense. Further identifying these, can help prevent a full email account compromise.



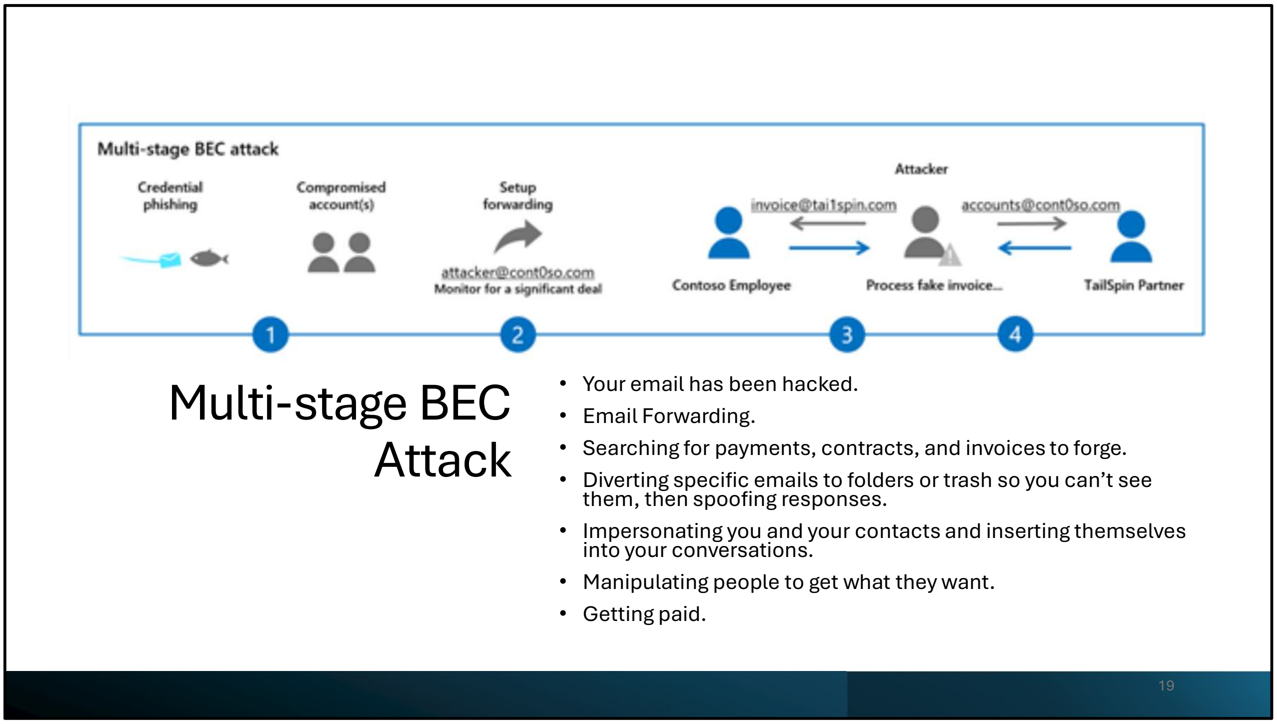
Classic BEC Attack

- NH town lost $2.3 million in email scam.
- Criminals took advantage of the transparent nature of public sector work.
- Spoofed vendor email
- Sent forged documents to change banking information.
- Got paid

https://statescoop.com/new-hampshire-town-lost-2-3-million-in-email-scam/

This happened to a small New Hampshire town in 2021. The town didn't realize until the vendor called regarding late payment. During the investigation, at least two more instances of BEC fraud were detected.

Remember, this is without access to your actual email account.



Multi-stage BEC Attack

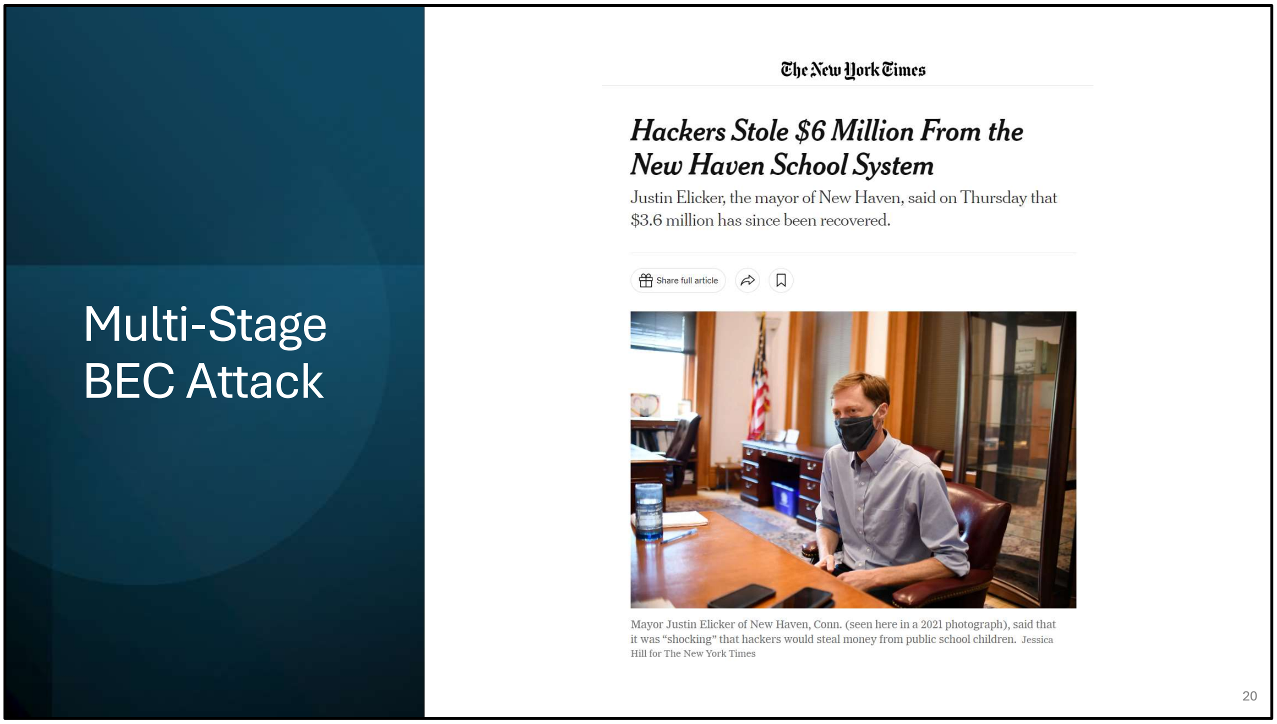
- Your email has been hacked.
- Email Forwarding.
- Searching for payments, contracts, and invoices to forge.
- Diverting specific emails to folders or trash so you can't see them, then spoofing responses.
- Impersonating you and your contacts and inserting themselves into your conversations.
- Manipulating people to get what they want.
- Getting paid.

https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/business-email-uncompromised-part-two/ba-p/2167246

Once a hacker has full access to an email account, the hacker can carry out complex long-term multi-stage BEC attacks.

A multi-stage BEC attack can be carried out once the hacker manages to actually gain access to your email account.
Usually, their first step is to set-up email forwarding. This way they can monitor your conversations to determine their best course of action.
They will also search your email for certain key terms like contract, payment, or invoice and figure out how to get paid.
They may divert emails from particular people into a folder so you don't see them.
They will send emails using your email address, which will of course go undetected by all of the controls previously mention to detect spoofing.

How can you tell this is happening, and what can you do about it?



Multi-Stage BEC Attack

The New York Times

Hackers Stole $6 Million From the New Haven School System

Justin Elicker, the mayor of New Haven, said on Thursday that $3.6 million has since been recovered.

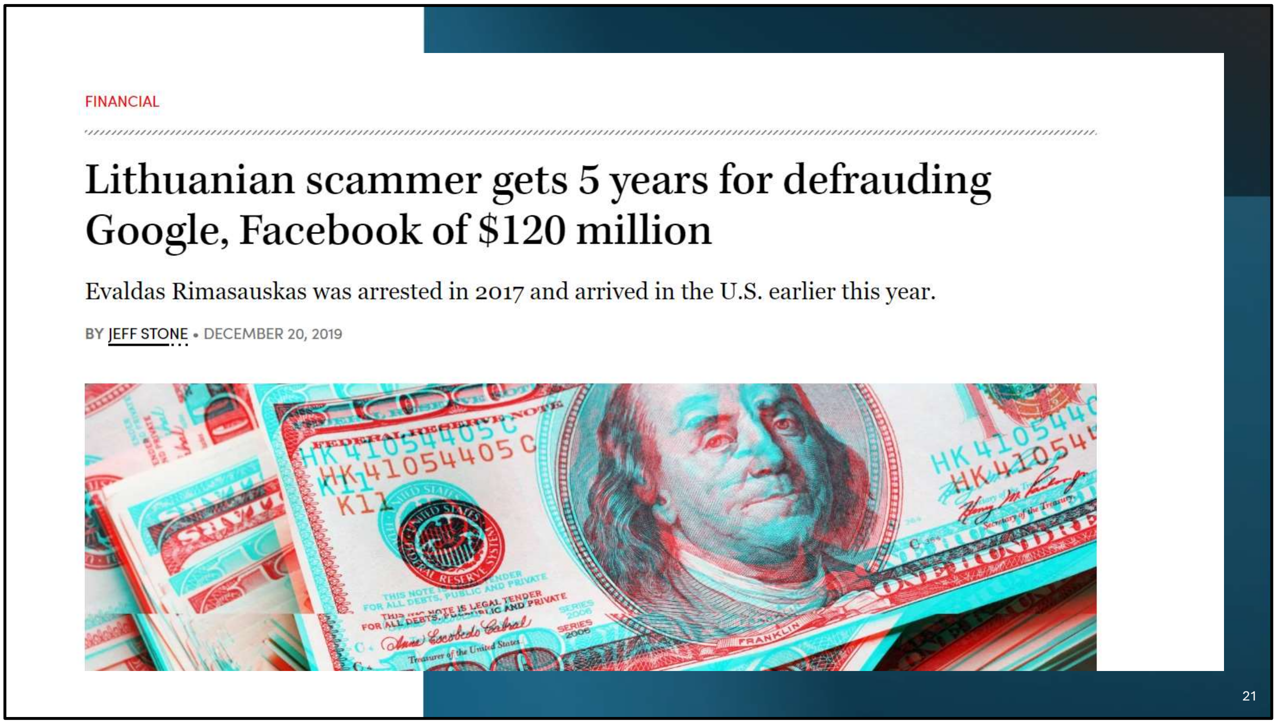
Share full article

Mayor Justin Elicker of New Haven, Conn. (seen here in a 2021 photograph), said that it was "shocking" that hackers would steal money from public school children. Jessica Hill for The New York Times

20

https://www.nytimes.com/2023/08/10/nyregion/new-haven-schools-hackers.html

The hackers appear to have gained access to the email account of the school system's chief operating officer and began to monitor conversations among the school official, vendors and the city's finance office,
The hackers impersonated the school official and vendors in order to divert the school's money to fraudulent accounts.
Six payments were made, totaling about $6 million before the school district realized it.
The incident was discovered when the real vendor called requesting payment.
About half was recouped.



FINANCIAL

Lithuanian scammer gets 5 years for defrauding Google, Facebook of $120 million

Evaldas Rimasauskas was arrested in 2017 and arrived in the U.S. earlier this year.

BY JEFF STONE • DECEMBER 20, 2019

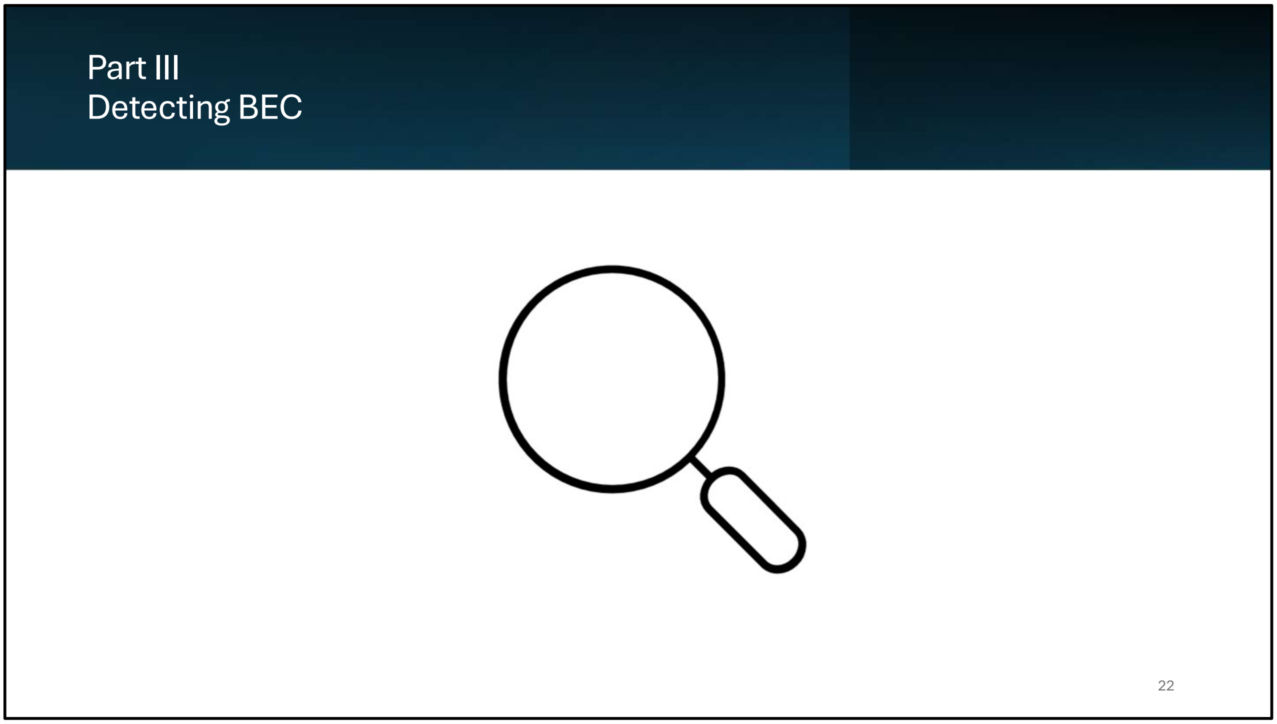
21

https://cyberscoop.com/facebook-google-scam-man-sentenced/

Don’t worry, it happens to the best of us. Even Google and Facebook got scammed.

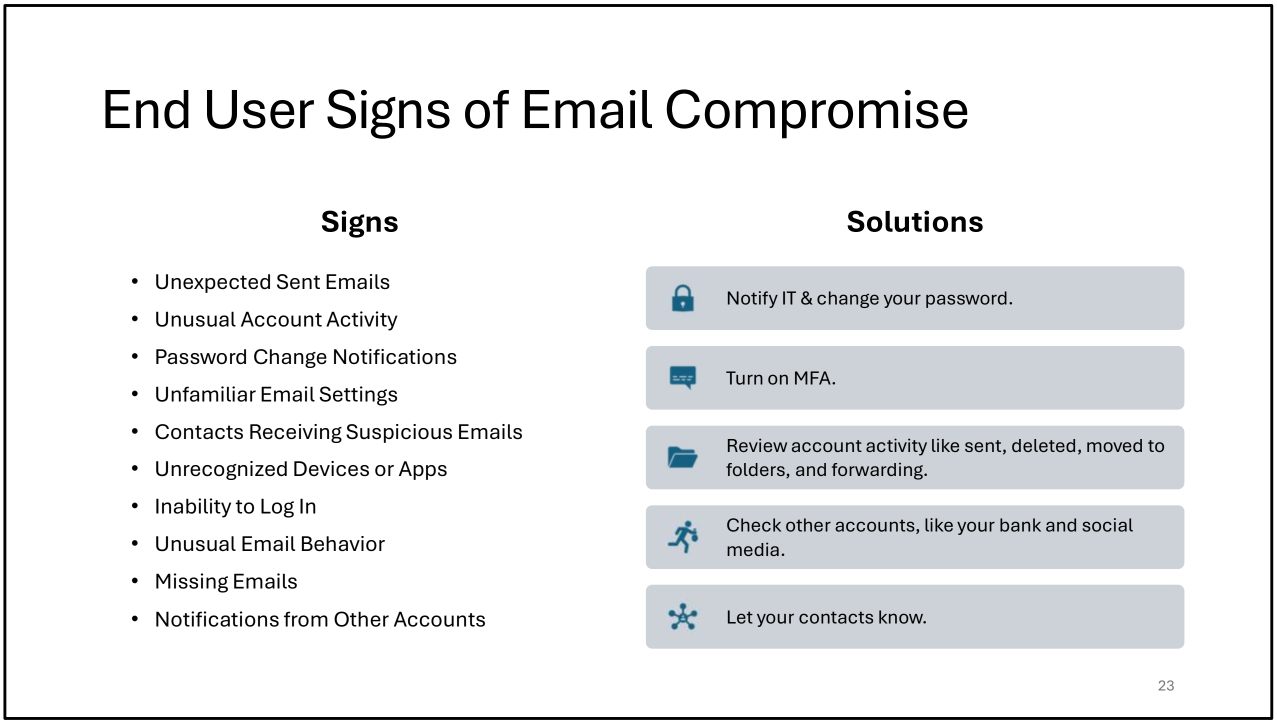
The defendant in this case created domains spoofing Quanta — a contractor that actually did build servers and other components for Facebook and Google — then sent fraudulent invoices, directing the companies’ employees to wire the fake Quanta real money. This went on for a two year period.

The discovery was made in the course of a regular audit. They reported it to law enforcement and were able to successfully prosecute the perpetrator.



Part III
Detecting BEC

There are signs that both end users and IT professionals can see to identify possible BEC activity.



End User Signs of Email Compromise

Signs

- Unexpected Sent Emails
- Unusual Account Activity
- Password Change Notifications
- Unfamiliar Email Settings
- Contacts Receiving Suspicious Emails
- Unrecognized Devices or Apps
- Inability to Log In
- Unusual Email Behavior
- Missing Emails
- Notifications from Other Accounts

Solutions

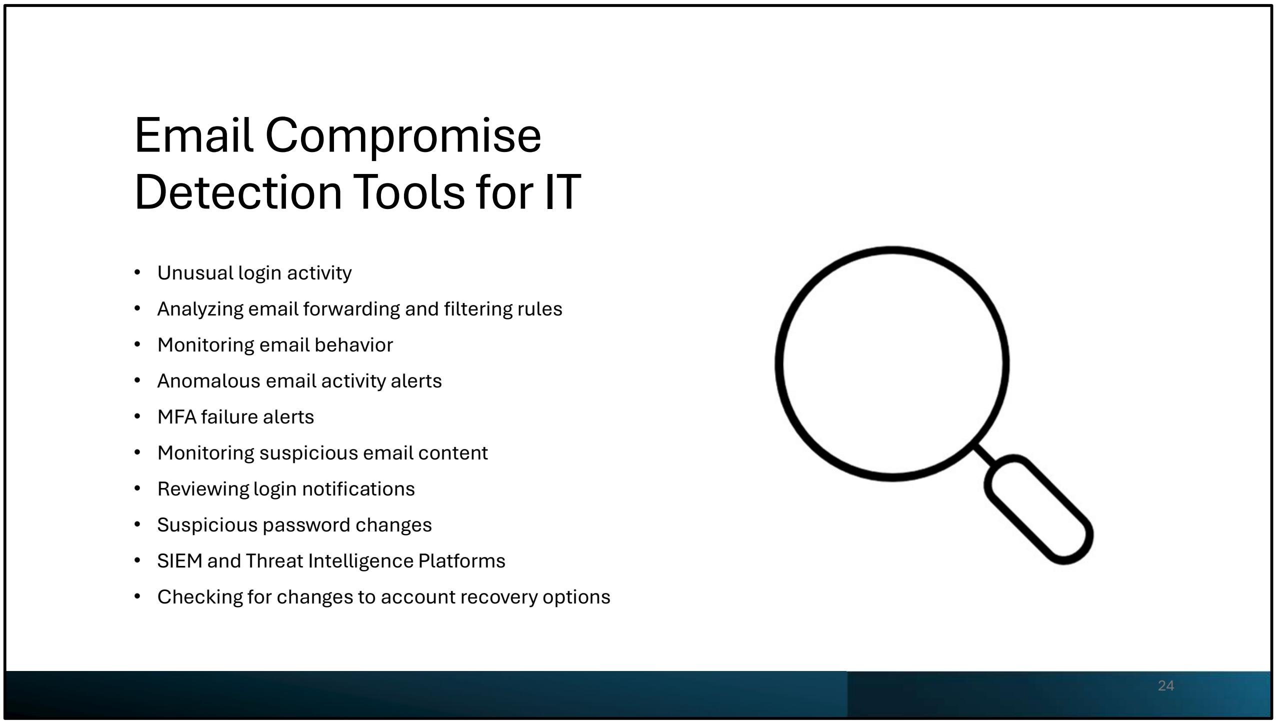
- Notify IT & change your password.
- Turn on MFA.
- Review account activity like sent, deleted, moved to folders, and forwarding.
- Check other accounts, like your bank and social media.
- Let your contacts know.

https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account?toc=%2Fmicrosoft-365%2Fbusiness-premium%2Ftoc.json&bc=%2Fmicrosoft-365%2Fbusiness-premium%2Fbreadcrumb%2Ftoc.json&view=o365-worldwide#symptoms-of-a-compromised-microsoft-email-account

1. Unexpected Sent Emails: Check your "Sent" folder or "Outbox" for emails you didn't send. Hackers may use your account to send spam or phishing emails to your contacts.
2. Unusual Account Activity: Logins from unfamiliar locations, devices, or IP addresses. Most email providers allow you to view recent login activity to spot suspicious access.
3. Password Change Notifications: Notifications about password changes or account recovery information updates that you didn’t initiate.
4. Unfamiliar Email Settings: Changes to your email settings, such as new email forwarding rules, filters, or auto-replies. Hackers often set up email forwarding to receive copies of your emails.
5. Contacts Receiving Suspicious Emails: Reports from your contacts about

receiving strange or suspicious emails from your address. This could indicate that your account is being used to spread spam or phishing.
6. Unrecognized Devices or Apps Connected to Your Account: Check for unfamiliar devices or third-party apps that have been granted access to your email account. This can often be found in your account's security settings.
7. Inability to Log In: If you suddenly can't access your account despite entering the correct password, it may have been compromised, and the hacker could have changed your login credentials.
8. Unusual Email Behavior: Look out for strange behavior such as emails being marked as read when you haven't read them, or drafts being saved that you didn't write.
9. Missing Emails: Emails that you know you received but can no longer find. Hackers sometimes delete or archive emails to cover their tracks.
10. Notifications from Other Accounts: Alerts from other services (like social media or bank accounts) about password resets or suspicious login attempts that could indicate your email is being used to access those accounts.

If you notice any of these signs, it's crucial to act quickly by securing your account, changing your passwords, enabling multi-factor authentication (MFA), and reviewing your account activity and security settings.



Email Compromise Detection Tools for IT

- Unusual login activity
- Analyzing email forwarding and filtering rules
- Monitoring email behavior
- Anomalous email activity alerts
- MFA failure alerts
- Monitoring suspicious email content
- Reviewing login notifications
- Suspicious password changes
- SIEM and Threat Intelligence Platforms
- Checking for changes to account recovery options

https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account?toc=%2Fmicrosoft-365%2Fbusiness-premium%2Ftoc.json&bc=%2Fmicrosoft-365%2Fbusiness-premium%2Fbreadcrumb%2Ftoc.json&view=o365-worldwide#symptoms-of-a-compromised-microsoft-email-account

IT departments use several tools and techniques to detect compromised email accounts.

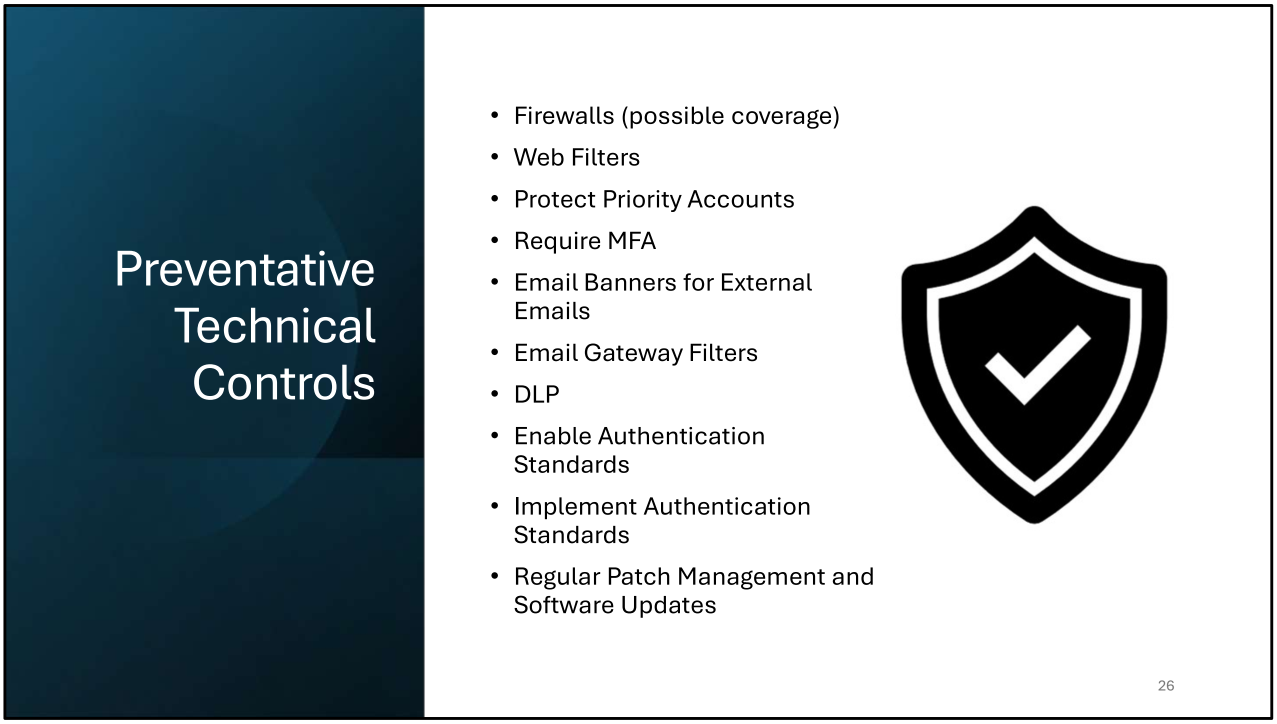
1. Monitoring Unusual Login Activity: Sudden logins from unusual countries or multiple failed login attempts can signal a compromised account.
2. Analyzing Email Forwarding and Filtering Rules: Unusual email forwarding or filter settings are a common indicator of a compromised email account.
3. Email Behavior Monitoring Tools: Anomalous behavior, such as sending out large volumes of phishing or spam emails, is a clear indication of an account breach.
4. Anomalous Email Activity Alerts: Real-time alerts provide IT teams with early warnings of potential compromises.
5. Multi-Factor Authentication (MFA) Failure Alerts: This helps detect when a hacker has the account password but cannot bypass the additional authentication layer.
6. Monitoring Suspicious Email Content: Outgoing spam or emails with harmful attachments often indicate that an account is under the control of hackers.

7. Reviewing Login Notifications: Unauthorized login alerts provide early detection, allowing IT teams to investigate further.
8. Suspicious Password Changes: Attackers often try to change passwords to lock out legitimate users after taking over an account.
9. SIEM and Threat Intelligence Platforms: SIEM tools provide comprehensive monitoring and correlation of data from various systems, helping detect sophisticated attacks.
10. Checking for Changes to Account Recovery Options: Changes to recovery options often indicate that a hacker is trying to take control of the account permanently.

By using a combination of these methods, IT departments can effectively detect email account compromises early and take action to prevent further damage. We will get into specific details in a minute. But first let's review how we can prevent email compromise in the first place.

Part IV
Preventing BEC

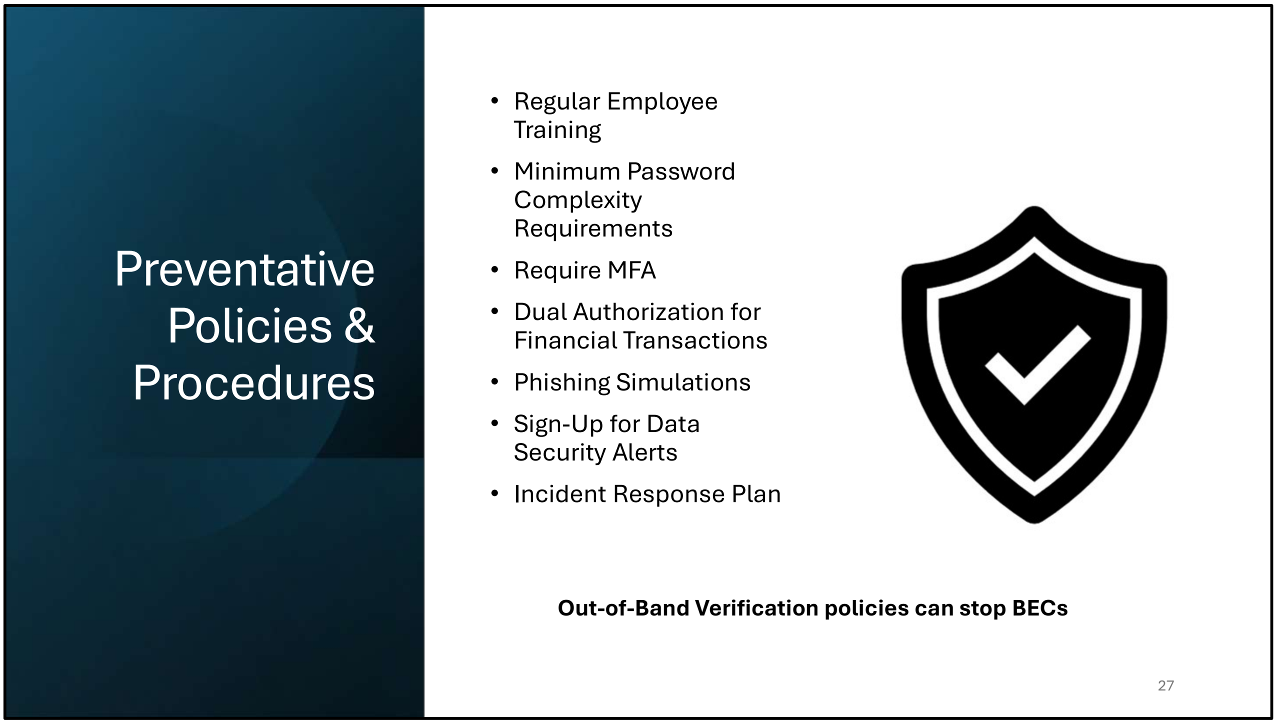
Obviously the main goal is to prevent a BEC attack in the first place. Preventing BEC attacks is a three-prong approach that includes technology, policies & procedures, and people.



Preventative Technical Controls

- Firewalls (possible coverage)
- Web Filters
- Protect Priority Accounts
- Require MFA
- Email Banners for External Emails
- Email Gateway Filters
- DLP
- Enable Authentication Standards
- Implement Authentication Standards
- Regular Patch Management and Software Updates

Firewalls block suspicious Ips
Web filters – Block fake login pages that mimic legitimate platforms
Priority Accounts – keep them protected
MFA – helps to mitigate the risk that hackers can access accounts even if they have login information
Emil banners for external emails – may help with spoofed internal emails
Email Gateway filters – to filter out emails with known phishing attempt indicators
Data Loss Prevention - if available
Implement SPF, DKIM, DMARC
Patch management and software updates – keeping things up to date will reduce vulnerabilities



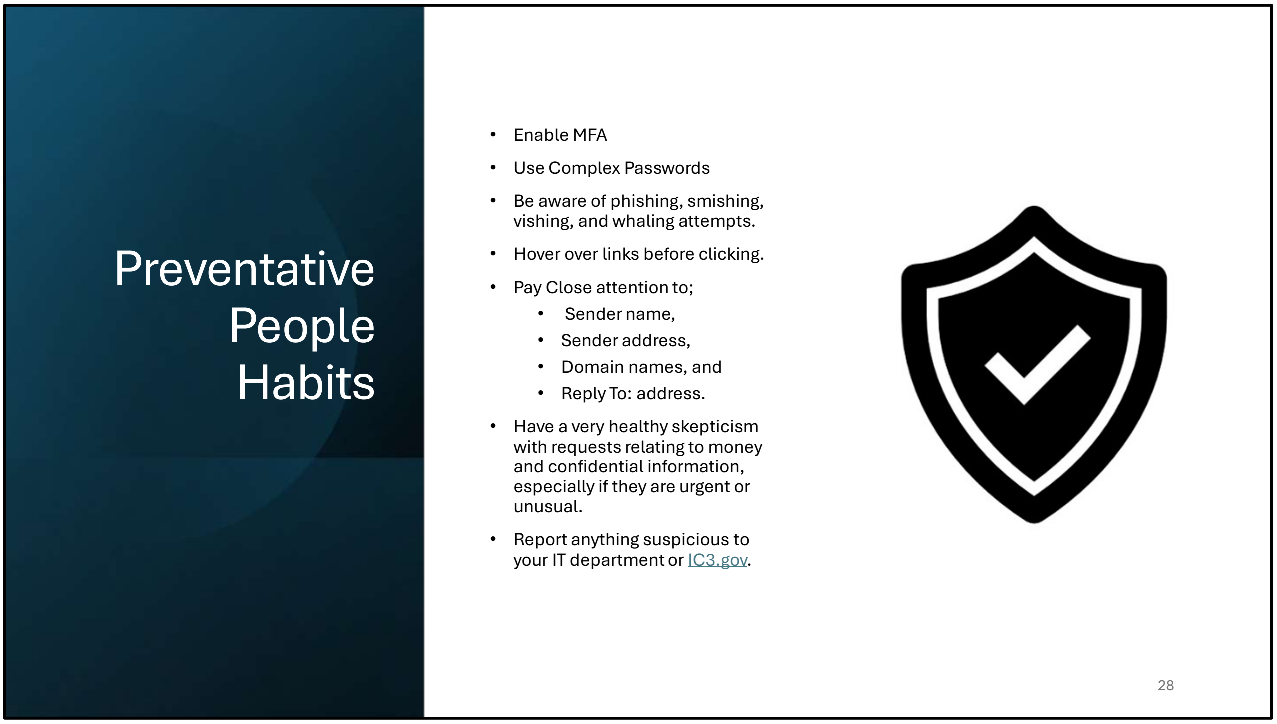
Preventative Policies & Procedures

- Regular Employee Training
- Minimum Password Complexity Requirements
- Require MFA
- Dual Authorization for Financial Transactions
- Phishing Simulations
- Sign-Up for Data Security Alerts
- Incident Response Plan

Out-of-Band Verification policies can stop BECs

27

Regular Employee Training: Educate employees on identifying and reporting phishing attempts, suspicious emails, and other social engineering tactics. Regular training sessions and simulated phishing exercises can improve vigilance.
Establish Dual Authorization for Financial Transactions: Require multiple approvals for wire transfers and changes to payment details. Implement a verification process, such as a phone call to a known contact, to confirm requests.
Use Out-of-Band Verification: Verifying payment requests or sensitive information changes through a separate communication channel (e.g., a phone call) helps confirm legitimacy.
•**Phishing Simulations** – helps employees understand what to look for to prevent social engineering tactics.
•Data Security Alerts -
•**Incident Response Plan** – the ability to quickly detect, contain, and respond to email compromises will mitigate potential damage.



Preventative People Habits

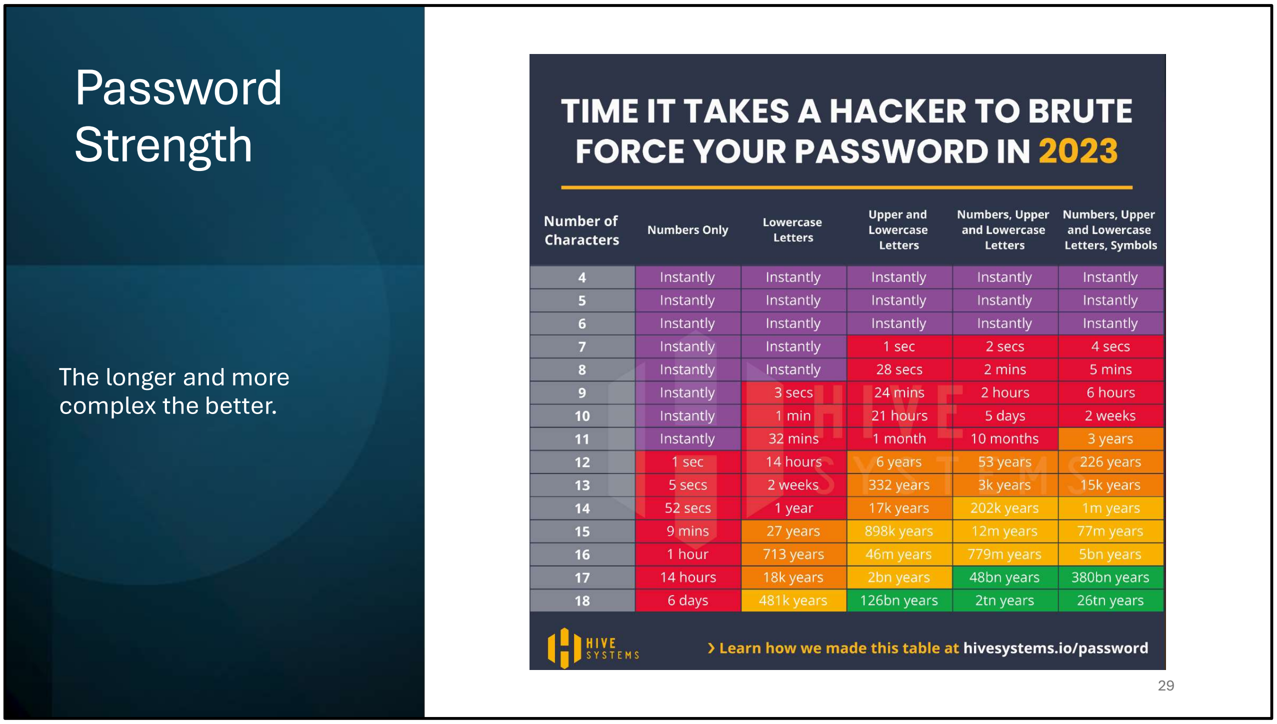
- Enable MFA
- Use Complex Passwords
- Be aware of phishing, smishing, vishing, and whaling attempts.
- Hover over links before clicking.
- Pay Close attention to;
  - Sender name,
  - Sender address,
  - Domain names, and
  - Reply To: address.
- Have a very healthy skepticism with requests relating to money and confidential information, especially if they are urgent or unusual.
- Report anything suspicious to your IT department or IC3.gov.

Enable Multi-Factor Authentication (MFA): Ensure that your email accounts are protected by MFA, which requires not just a password but also a second form of verification, like a code sent to your phone. This makes it much harder for attackers to gain access, even if they steal your password.

Use Strong, Unique Passwords:
•**Create Strong Passwords:** Use complex passwords that are at least 12 characters long and include a mix of letters, numbers, and symbols. Avoid using the same password across multiple sites.
•**Password Manager:** Consider using a password manager to generate and store strong, unique passwords for each of your accounts.

Be Aware of Phishing Attempts:
•**Recognize and Avoid Phishing Emails:** Be suspicious of unsolicited emails, especially those that urge immediate action or ask you to click on links or open attachments. Look for red flags like poor grammar, unusual requests, or unfamiliar email addresses.

•**Hover Over Links:** Before clicking on any link in an email, hover your cursor over it to check the actual URL. If it doesn’t match the supposed sender or looks suspicious, don’t click it.



Password Strength

The longer and more complex the better.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

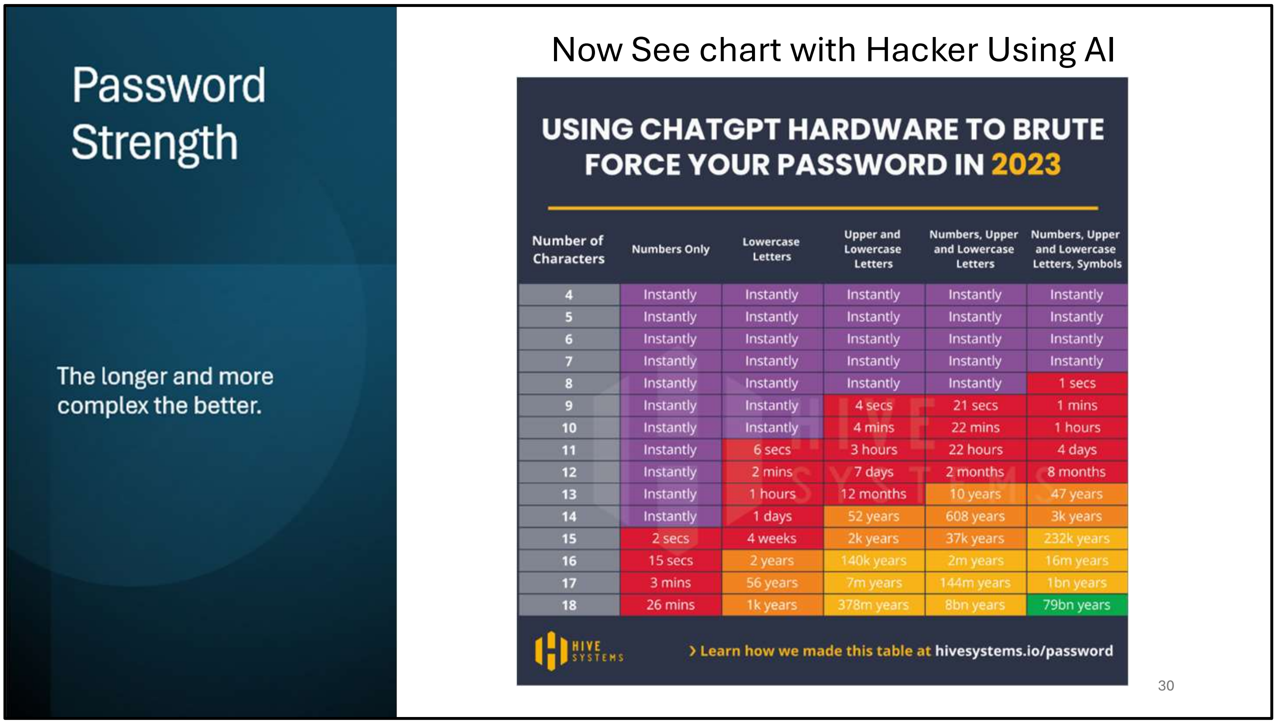
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

> Learn how we made this table at hivesystems.io/password

29

https://www.reddit.com/r/dataisbeautiful/comments/12qmvlw/oc_i_updated_our_famous_password_table_for_2023/#lightbox



Password Strength

The longer and more complex the better.

Now See chart with Hacker Using AI

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

HIVE SYSTEMS

> Learn how we made this table at hivesystems.io/password

30

https://www.reddit.com/r/dataisbeautiful/comments/12qmvlw/oc_i_updated_our_famous_password_table_for_2023/#lightbox

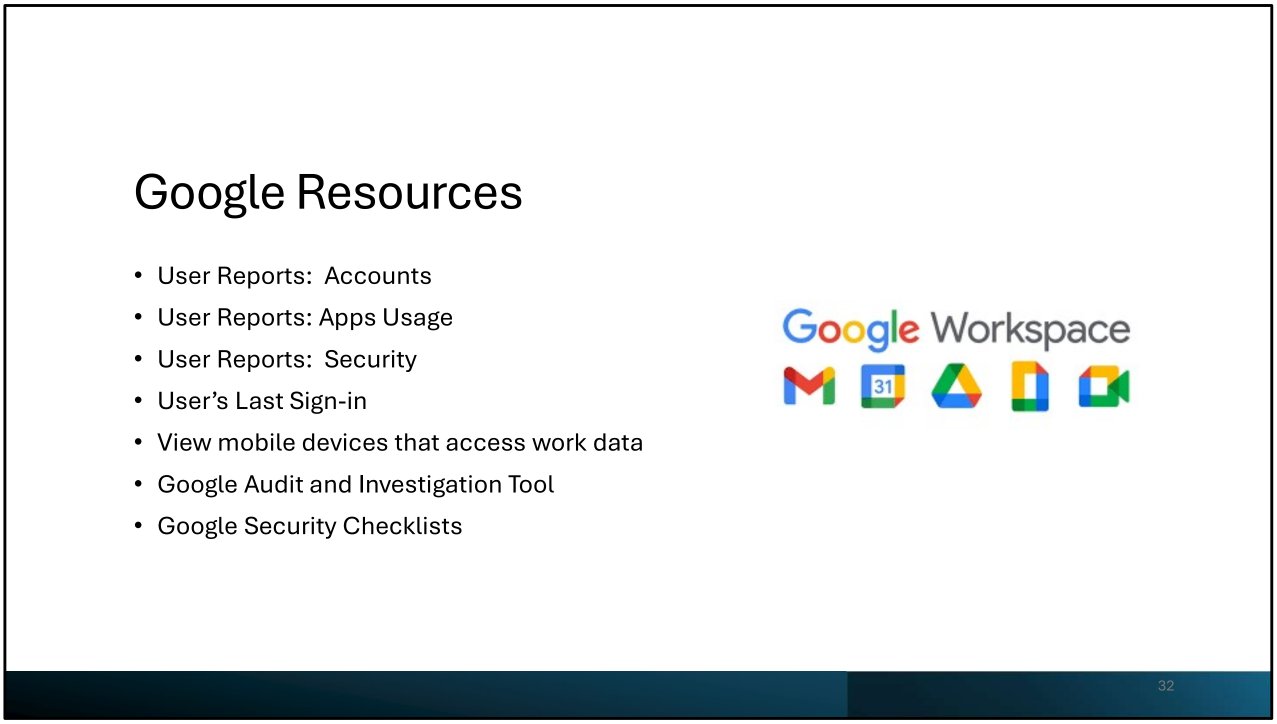
https://www.hivesystems.com/password-table

Part V
Investigating BEC

Google Workspace Microsoft 365

Investigating BEC attacks. If you've managed to not fall asleep yet, you are officially IT enthusiast.

Most people are probably operating in either Google Workspace or Microsoft…



Google Resources

- User Reports: Accounts
- User Reports: Apps Usage
- User Reports: Security
- User's Last Sign-in
- View mobile devices that access work data
- Google Audit and Investigation Tool
- Google Security Checklists

Google Workspace
31

https://support.google.com/a/topic/9026833?hl=en&ref_topic=4490889&sjid=10413781363690091015-NA

Check user or admin activity

User reports: Accounts: View users' account status and activity

User reports: Apps usage:

Emails sent over a specific period.
How many files users create and share.
Which users are near their Drive storage limits.
The number of search queries from different types of devices.

User reports: Security: View your users' account settings and exposure to security risks

View your users' last sign-in: check when a user last signed in to their account.

Note: Data lag time from a couple of hours up to 3 days.

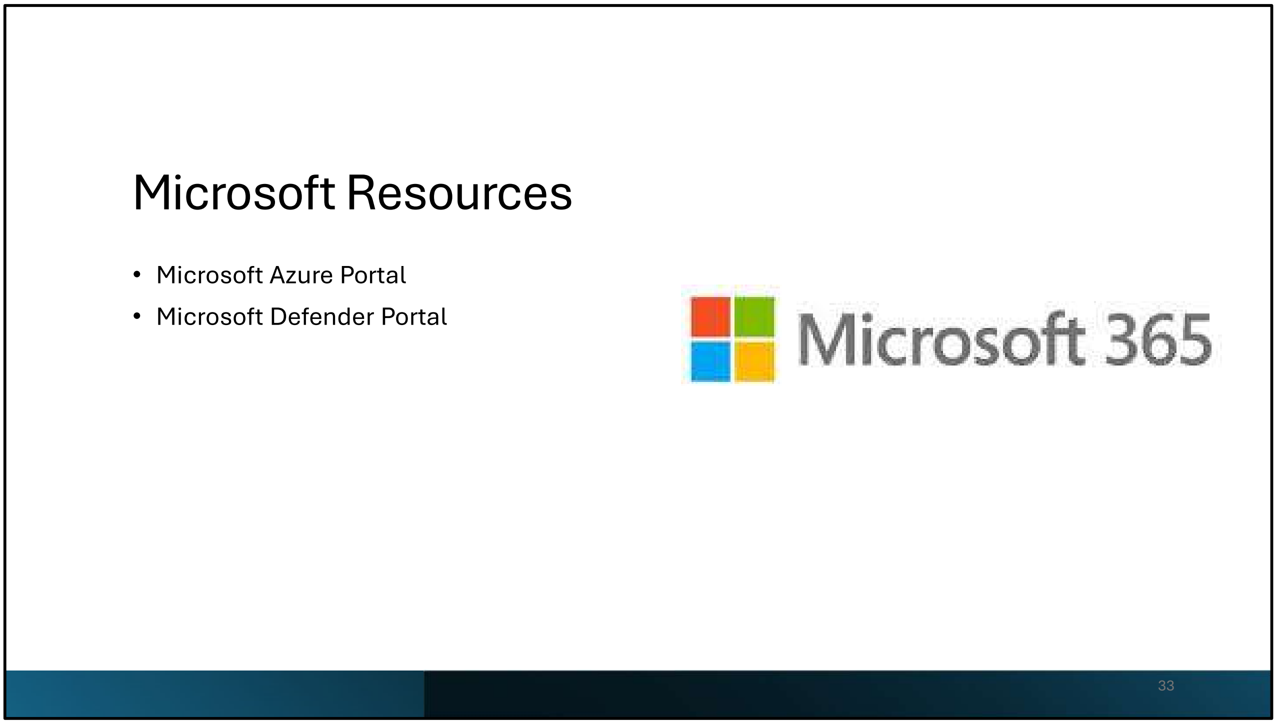
Check device activity: **View mobile devices that access work data**

About the audit and investigation tool

In your Google Admin console, you can use the *audit and investigation tool* to review user and administrator activity in your organization. You can use the information to track users and admins, and for security purposes.

Under 100 users:
https://support.google.com/a/answer/9211704?sjid=15565943473449761275-NA

100+ users:
https://support.google.com/a/answer/7587183?hl=en&ref_topic=7559287&sjid=15565943473449761275-NA#zippy=%2Caccounts



Microsoft Resources

- Microsoft Azure Portal
- Microsoft Defender Portal

Microsoft 365

Microsoft Defender for Office 365 - Automatically checks email authentication, detects spoofing, and quarantines or sends suspicious emails to junk folders. It can also use AI to model normal email patterns and flag unusual activity.

Azure Identity Protection - Helps protect against compromised identities, account takeover, and misuse of privileges.

Microsoft Entra logs - Can be integrated with other tools, like Microsoft Sentinel and Azure Monitor, to monitor and audit logs for suspicious behavior.

Microsoft Entra admin center - Includes sign-in logs and other risk reports that can be examined for IP address, sign-in locations, sign-in times, and sign-in success or failure.

The Microsoft Defender portal has several tools to help prevent business email compromise, including:

Anti-phishing policies: Configure settings for impersonation protection, mailbox intelligence, and phishing thresholds.

Campaign views: Use machine learning to identify and analyze messages that may be part of a phishing attack.

Attack simulation training: Create fake phishing messages to send to internal users as a training tool.

Exchange Online Protection: Analyzes and blocks messages based on sender reputation and email authentication methods.

Safe attachments: Tests attachments to determine their safety.

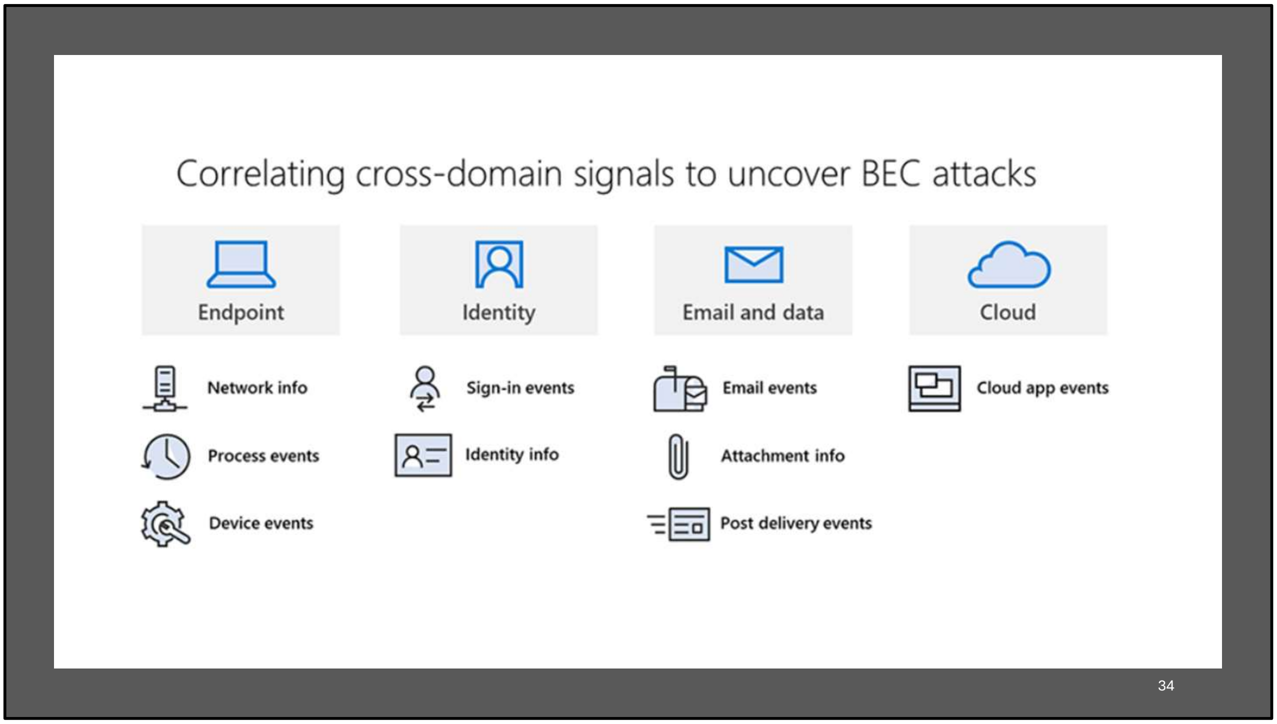
Defender for Endpoint: Manages devices connected to the network.

Defender for Identity: Detects high-risk lateral movement and sudden account changes.

Microsoft Defender for Cloud Apps: Detects anomalous behavior and reports it to the security team.

Hunting: Build custom detection rules to hunt for specific threats.

Unified audit logs: Filter logs for activity using a date range.

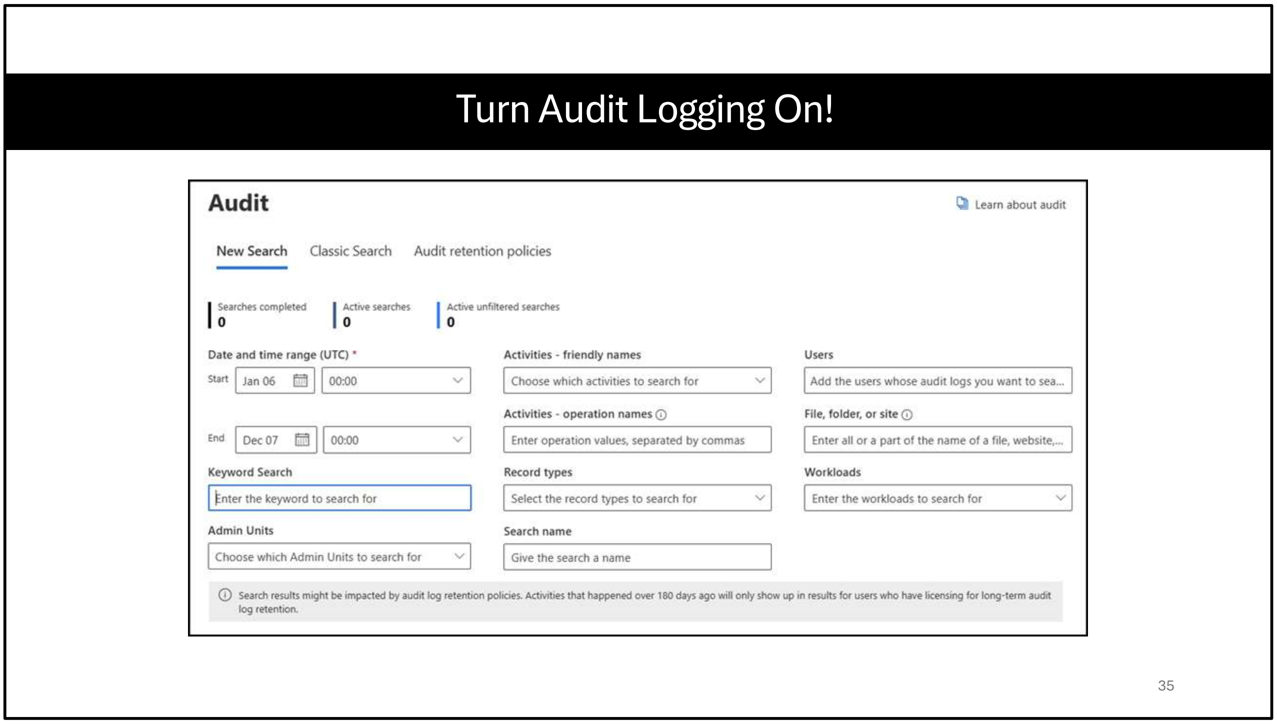


Correlating cross-domain signals to uncover BEC attacks

Endpoint	Identity	Email and data	Cloud
Network info	Sign-in events	Email events	Cloud app events
Process events	Identity info	Attachment info	
Device events		Post delivery events	

https://www.microsoft.com/en-us/security/blog/2021/06/14/behind-the-scenes-of-business-email-compromise-using-cross-domain-threat-data-to-disrupt-a-large-bec-infrastructure/

Microsoft offers very robust BEC tools.



Turn Audit Logging On!

Audit

Learn about audit

New Search | Classic Search | Audit retention policies

Searches completed 0 | Active searches 0 | Active unfiltered searches 0

Date and time range (UTC) *

Start: Jan 06 | 00:00

End: Dec 07 | 00:00

Activities - friendly names: Choose which activities to search for

Activities - operation names: Enter operation values, separated by commas

Users: Add the users whose audit logs you want to sea...

File, folder, or site: Enter all or a part of the name of a file, website,...

Keyword Search: Enter the keyword to search for

Record types: Select the record types to search for

Workloads: Enter the workloads to search for

Admin Units: Choose which Admin Units to search for

Search name: Give the search a name

Search results might be impacted by audit log retention policies. Activities that happened over 180 days ago will only show up in results for users who have licensing for long-term audit log retention.

35

Source: https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/investigating-malicious-oauth-applications-using-the-unified/ba-p/4007172

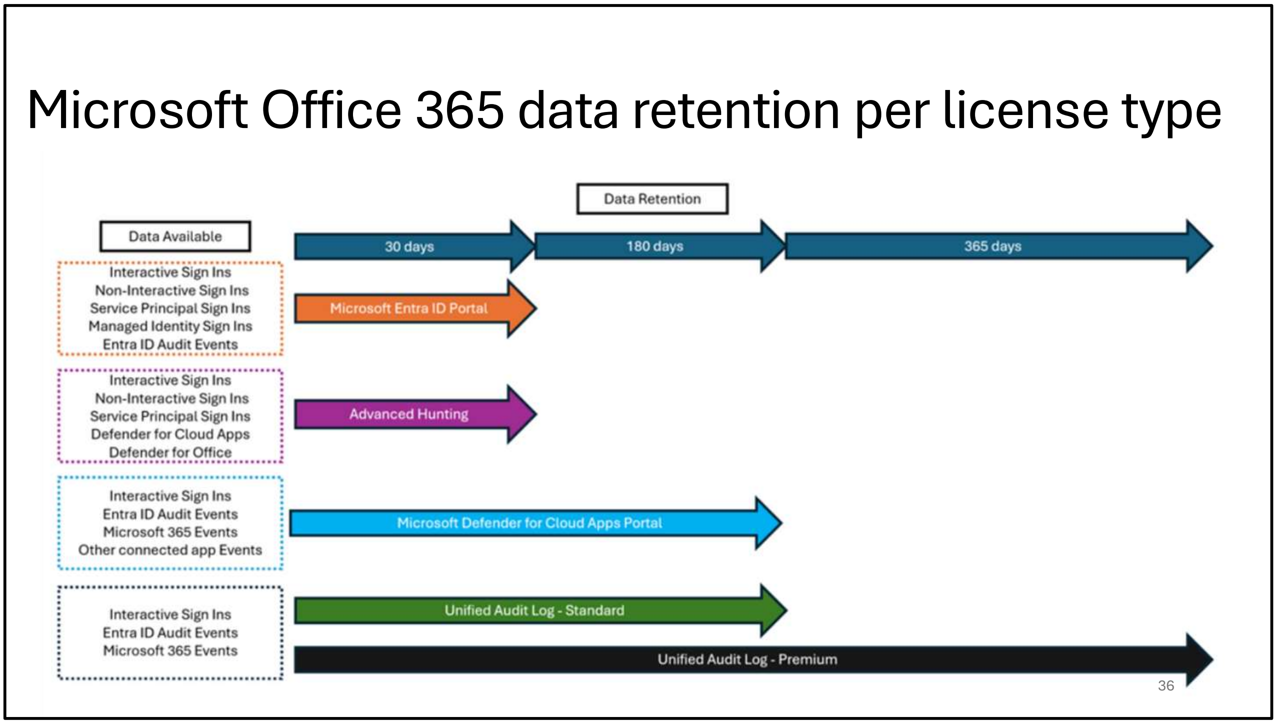
Turn on audit logging for all of your systems. Know how long the data is retained, back it up and store it as needed. Should a security event occur, this will be the only way to get any definitive answers.

Using the Audit search functionality, you can create custom searches to retrieve the relevant information from the Unified Audit Log.
This data can then be downloaded as a CSV file and analyzed to understand what happened.

Unified audit logs in the Microsoft Defender portal:
Filter the logs for activity using a date range that starts immediately before the suspicious activity occurred to today. Don't filter on specific activities during the search.

Microsoft Entra sign-in logs and other risk reports in the Microsoft Entra admin center:
Examine the values in these columns:

- Review IP address
- sign-in locations
- sign-in times
- sign-in success or failure



Microsoft Office 365 data retention per license type

Data Retention

Data Available

30 days

180 days

365 days

Interactive Sign Ins
Non-Interactive Sign Ins
Service Principal Sign Ins
Managed Identity Sign Ins
Entra ID Audit Events

Microsoft Entra ID Portal

Interactive Sign Ins
Non-Interactive Sign Ins
Service Principal Sign Ins
Defender for Cloud Apps
Defender for Office

Advanced Hunting

Interactive Sign Ins
Entra ID Audit Events
Microsoft 365 Events
Other connected app Events

Microsoft Defender for Cloud Apps Portal

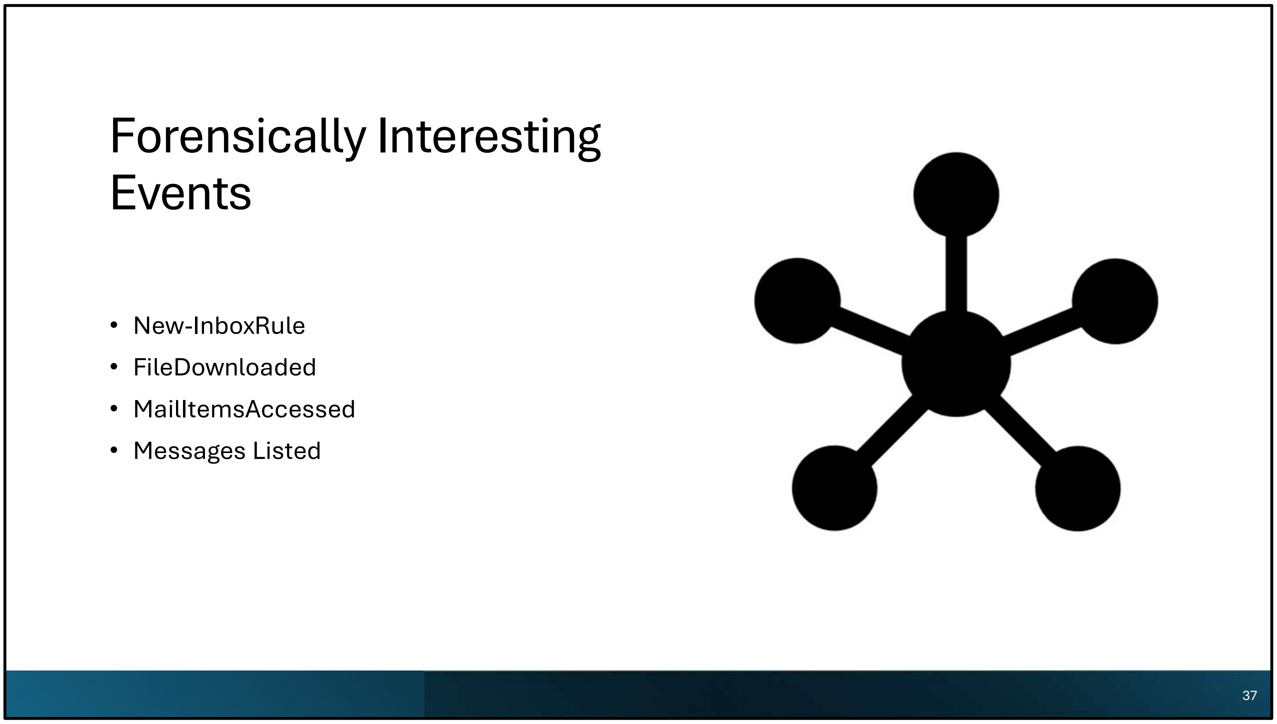
Interactive Sign Ins
Entra ID Audit Events
Microsoft 365 Events

Unified Audit Log - Standard

Unified Audit Log - Premium

36

Understand your data retention so you can run reports and backup as needed.



Forensically Interesting Events

- New-InboxRule
- FileDownloaded
- MailItemsAccessed
- Messages Listed

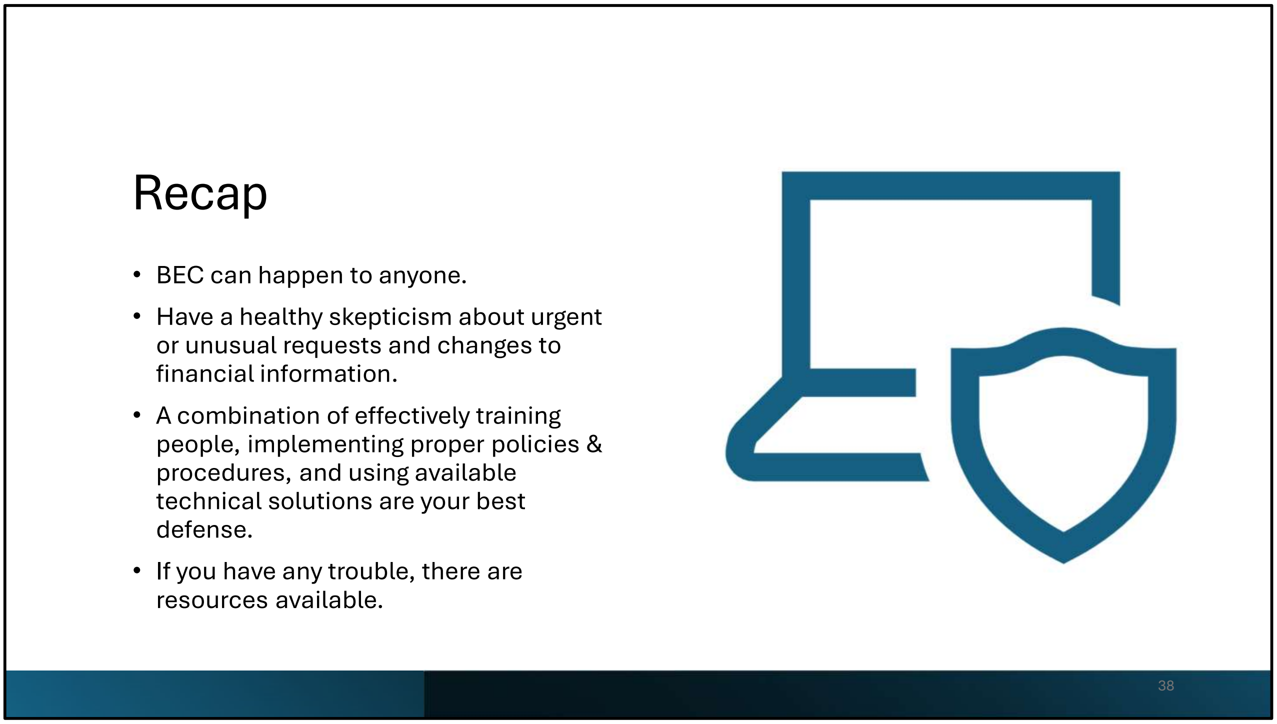
New-InboxRule: A mailbox owner or other user with access to the mailbox created an inbox rule in the Outlook web app. With these events Microsoft IR is interested in what actions the rule was taking, was it trying to hide emails with particular words or phrases, that may be an indicator of threat actor intent. If they are hiding emails related to invoices or payment, it may be a sign the threat actor is seeking financial gain through business email compromise.

FileDownloaded – This will show the filename and file path of file downloaded events, and the identity that triggered the action – whether that is a user or an application.

MailItemsAccessed – this event shows that an email within a mailbox in Exchange Online was accessed.

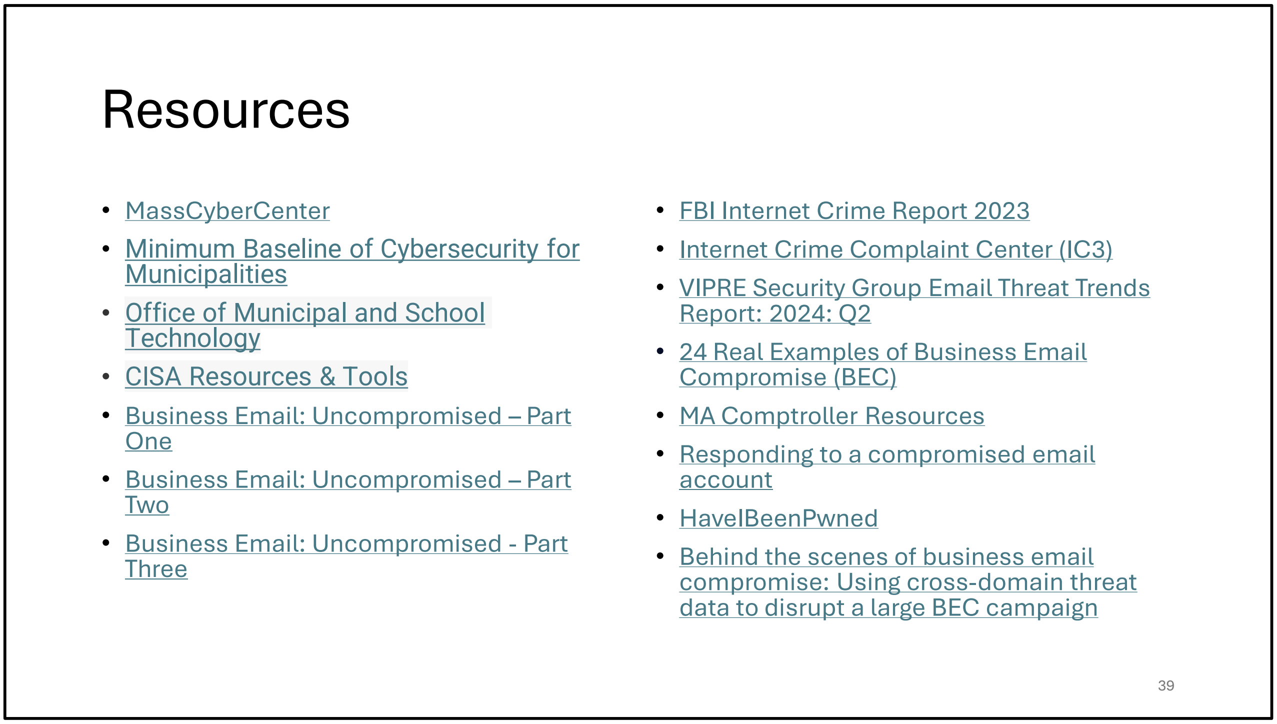
MessagesListed – When a Teams message is retrieved from the Microsoft Graph API, this event is logged. It is not logged when a message is listed from the Microsoft Teams client itself. Threat actors can use tooling they have created to interact directly with the Microsoft Graph API and access messages in bulk, the

MessagesListed event is valuable for understanding the impact of this kind of activity. Add service principal: This event is logged when a service principal is added to the tenant. If this is malicious activity during the investigation, then Microsoft IR pivots on that application to understand what other activities it completed, and what data and services it accessed. The ApplicationId, which is a guid, of the newly created application is a strong indicator of compromise.



Recap

- BEC can happen to anyone.
- Have a healthy skepticism about urgent or unusual requests and changes to financial information.
- A combination of effectively training people, implementing proper policies & procedures, and using available technical solutions are your best defense.
- If you have any trouble, there are resources available.



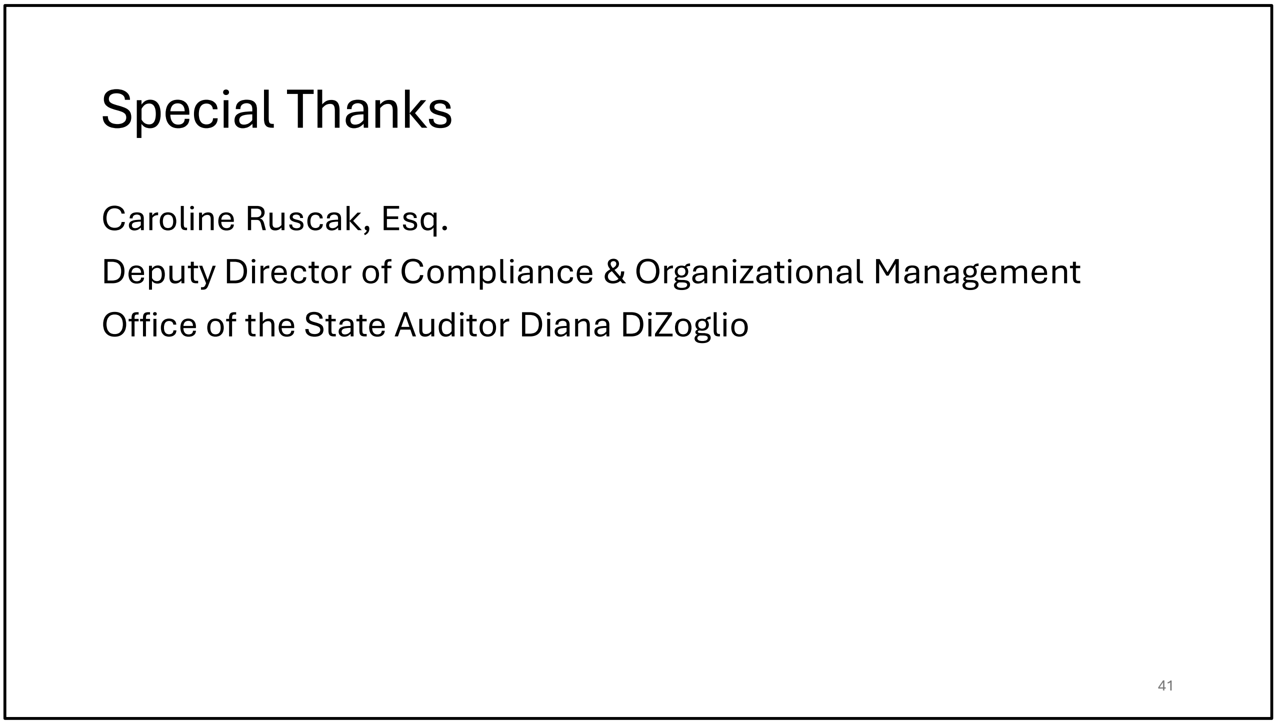
Resources

- MassCyberCenter
- Minimum Baseline of Cybersecurity for Municipalities
- Office of Municipal and School Technology
- CISA Resources & Tools
- Business Email: Uncompromised – Part One
- Business Email: Uncompromised – Part Two
- Business Email: Uncompromised - Part Three
- FBI Internet Crime Report 2023
- Internet Crime Complaint Center (IC3)
- VIPRE Security Group Email Threat Trends Report: 2024: Q2
- 24 Real Examples of Business Email Compromise (BEC)
- MA Comptroller Resources
- Responding to a compromised email account
- HaveIBeenPwned
- Behind the scenes of business email compromise: Using cross-domain threat data to disrupt a large BEC campaign

Questions

Contact Information

MassCyberCenter
at the MassTech Collaborative



Special Thanks

Caroline Ruscak, Esq.
Deputy Director of Compliance & Organizational Management
Office of the State Auditor Diana DiZoglio