ISSA Information Systems Security Association

Thought Leadership Web CONFERENCE

Combating Business Email Compromise & Email Account Compromise

February 19, 2020

Today’s web conference is generously sponsored by:

proofpoint®

https://www.proofpoint.com/

Combating Business Email Compromise & Email Account Compromise

Moderator

Lee Neely, Senior IT and Cybersecurity Professional, LLNL

Lee Neely is a senior IT and security professional at LLNL with over 30 years of extensive experience with a wide variety of technology and applications from point implementations to enterprise solutions. He currently leads LLNL's Entrust team and is the CSP lead for new technology adoption specializing in mobility. He teaches cyber security courses, and holds several security certifications including GMOB, GPEN, GWAPT, GAWN, CISSP, CISA, CISM and CRISC. He recently joined the ISSA International Board of Directors and is also the Treasurer for the CSA Boise chapter, and past President for the ISC2 Eastbay Chapter, Member of the SANS NewsBites Editorial Board and SANS Analyst.

You can keep up with Lee @lelandneely

Combating Business Email Compromise & Email Account Compromise

Speaker

Tanner Luxner, Product Marketing Manager, proofpoint

Tanner Luxner is a product marketing manager for Proofpoint, currently overseeing product marketing for Proofpoint's Email Fraud Defense, Threat Response and Proofpoint Essentials Solutions. Proofpoint helps organizations protect their people through an integrated, cloud-based suite of people-centric compliance and security solutions to help mitigate today’s security and compliance risks.

North Carolina county paid $2.5M to BEC scammers

$26.2B+

Direct losses worldwide
(June 2016 – July 2020)

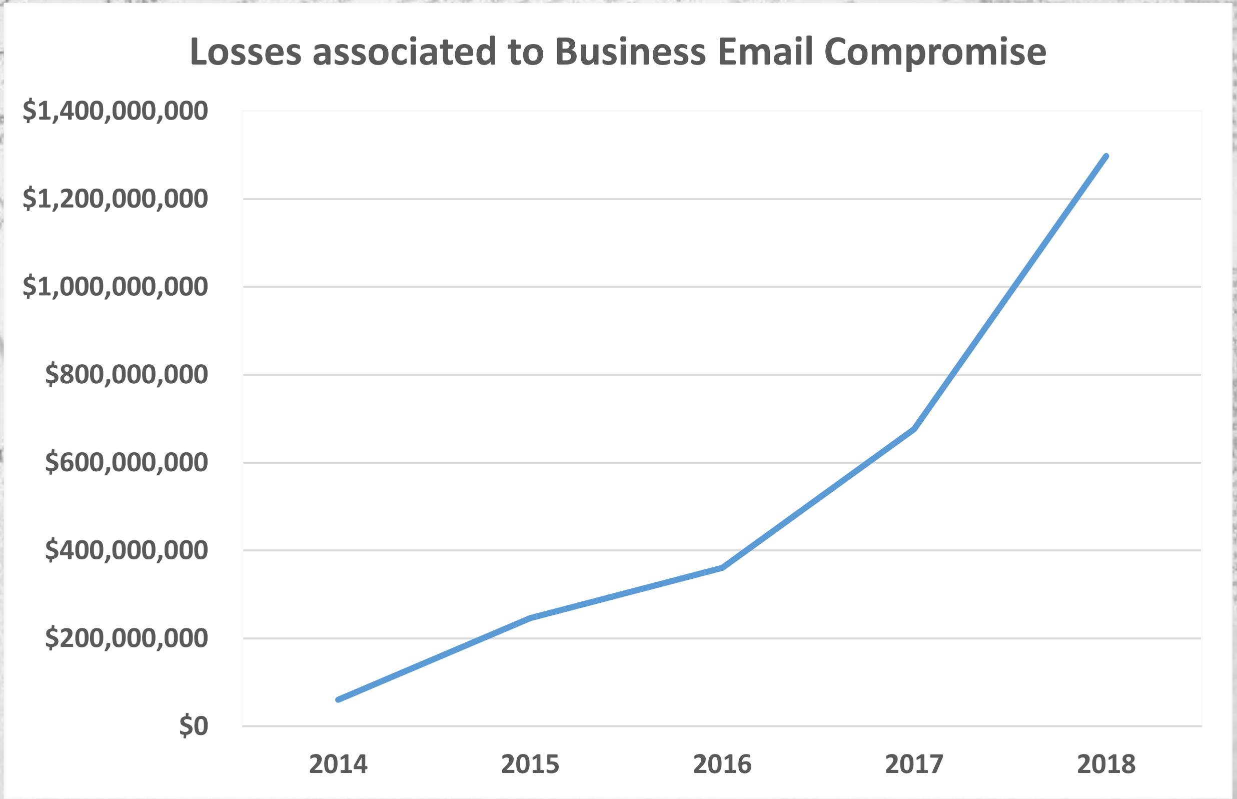
Source: FBI

- **BEC Scam Costs Media Giant Nikkei $29M**
- **BEC Fraudsters Divert $742,000 from Ocala City**
- **Texas School District Loses 2.3M in BEC Scam**
- **Town of Erie Paid $1M to BEC Scammers**

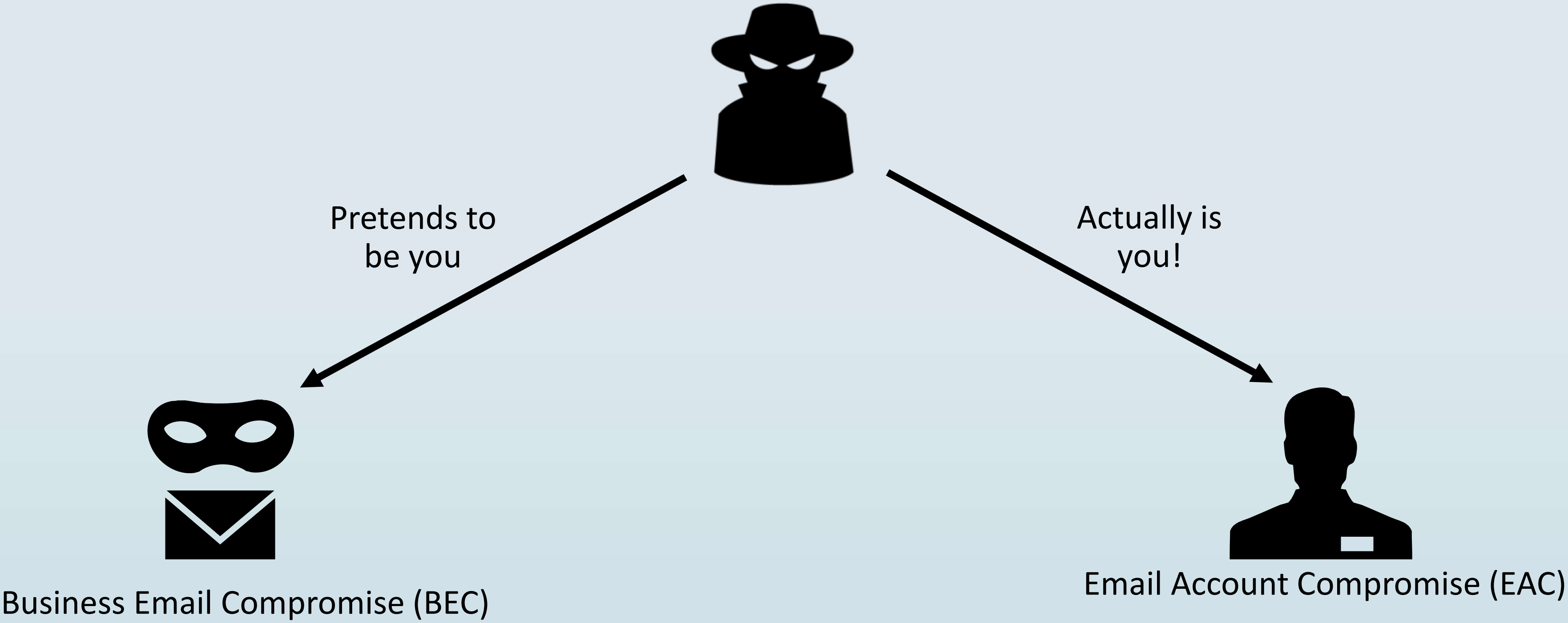
$1.7B

Associated to Business Email Compromise in 2019 alone

FBI



Email Fraud Leads to Two Main Threats



Pretends to be you

Actually is you!

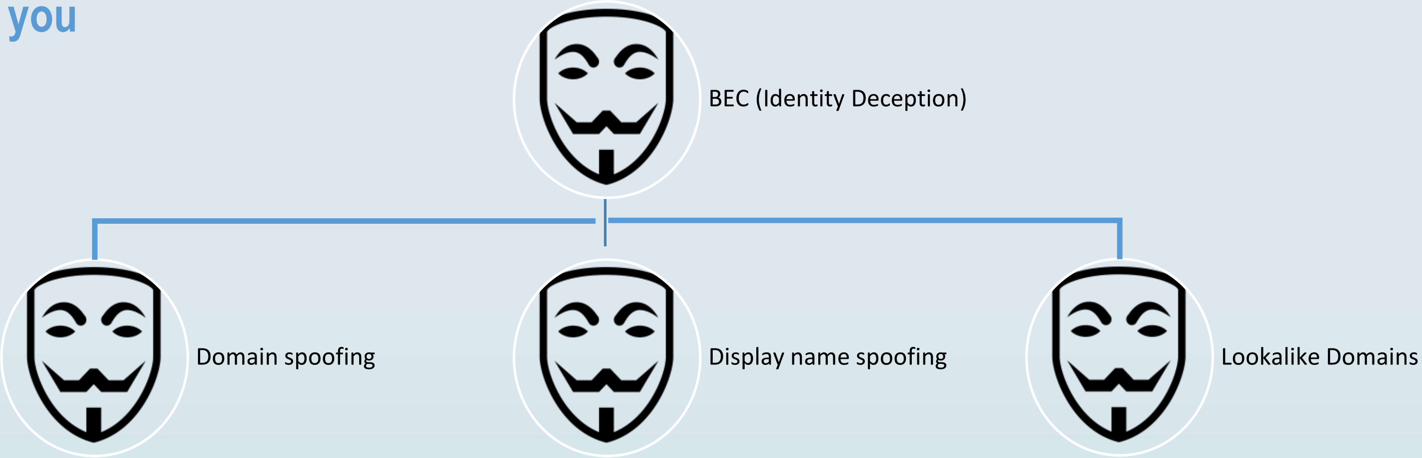
Business Email Compromise (BEC)

Email Account Compromise (EAC)

What’s BEC

Business Email Compromise (BEC)

Pretend to be you



BEC (Identity Deception)

Domain spoofing

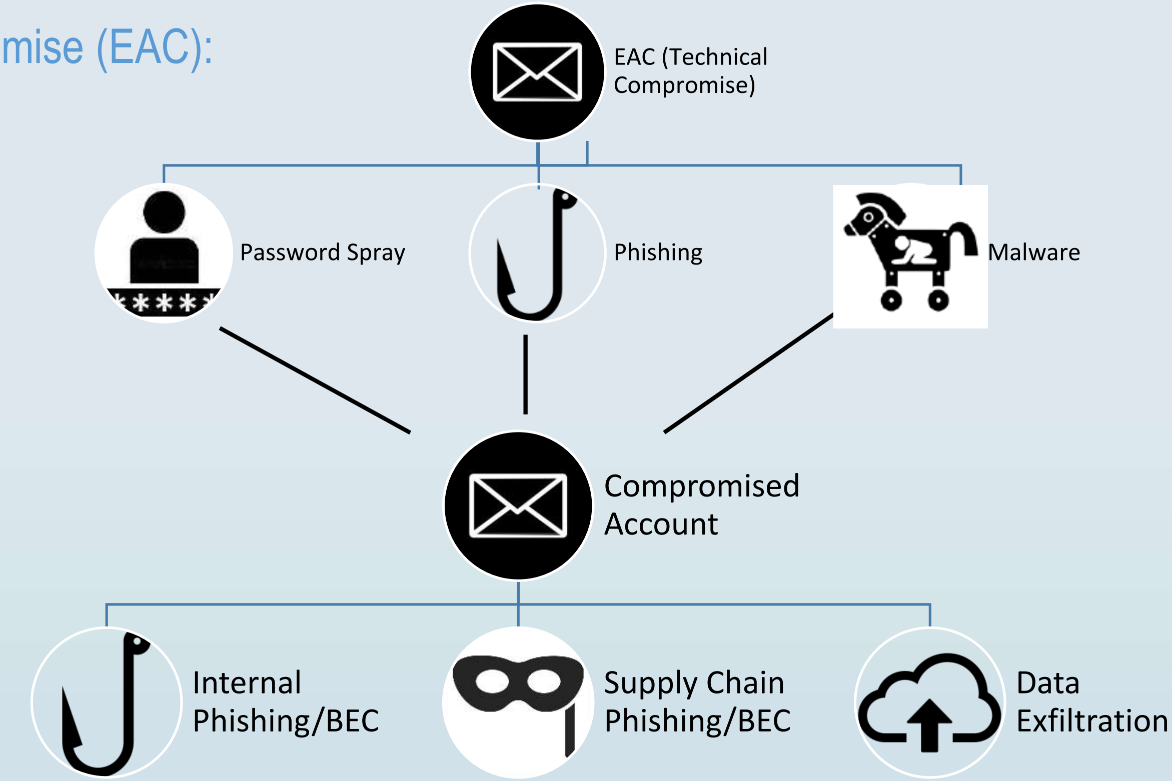
Display name spoofing

Lookalike Domains

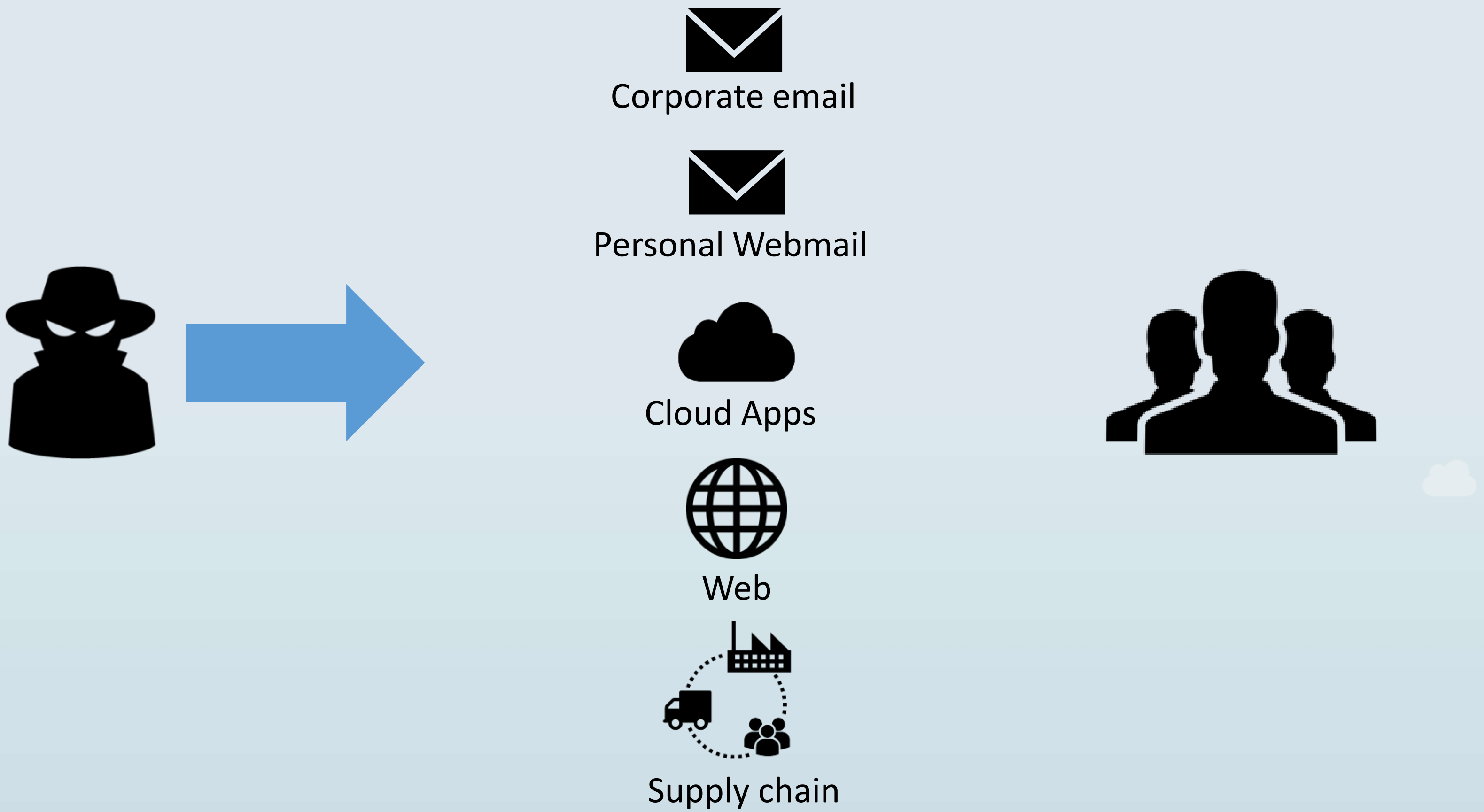
What’s BEC/EAC?

Email Account Compromise (EAC):

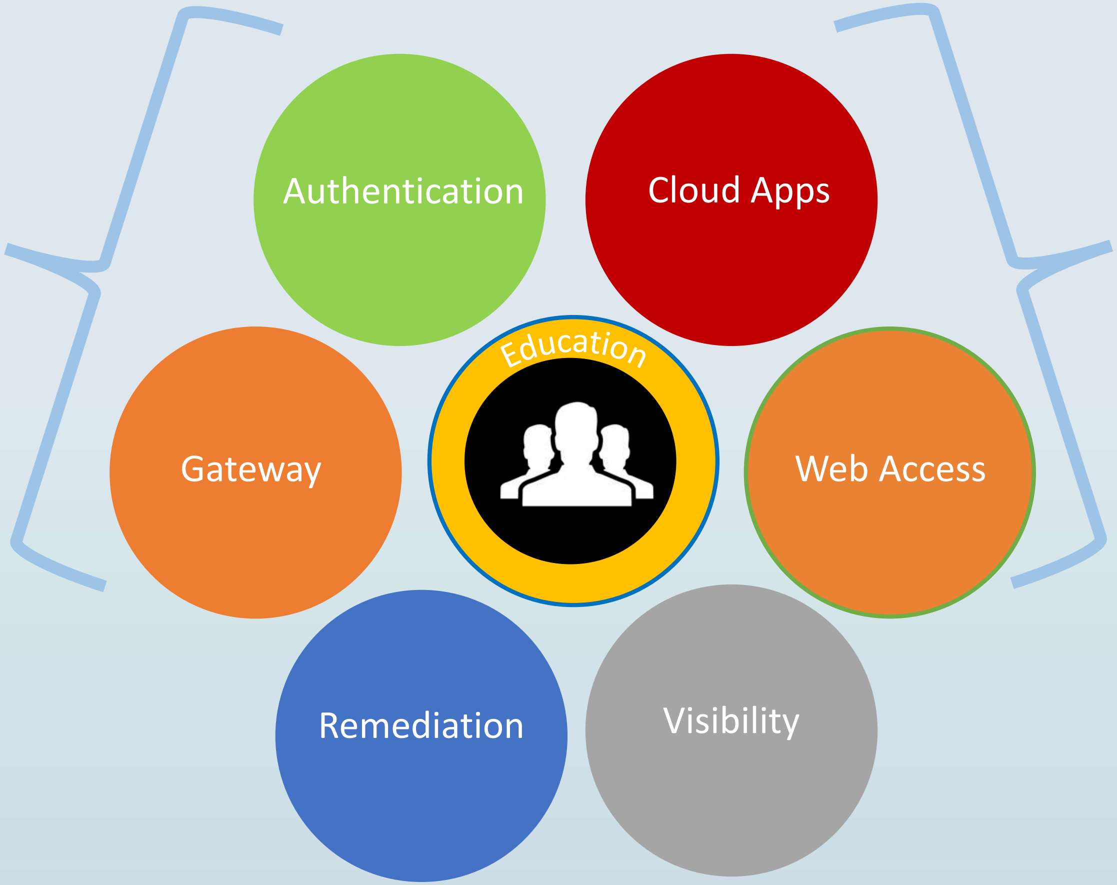
Actually become you



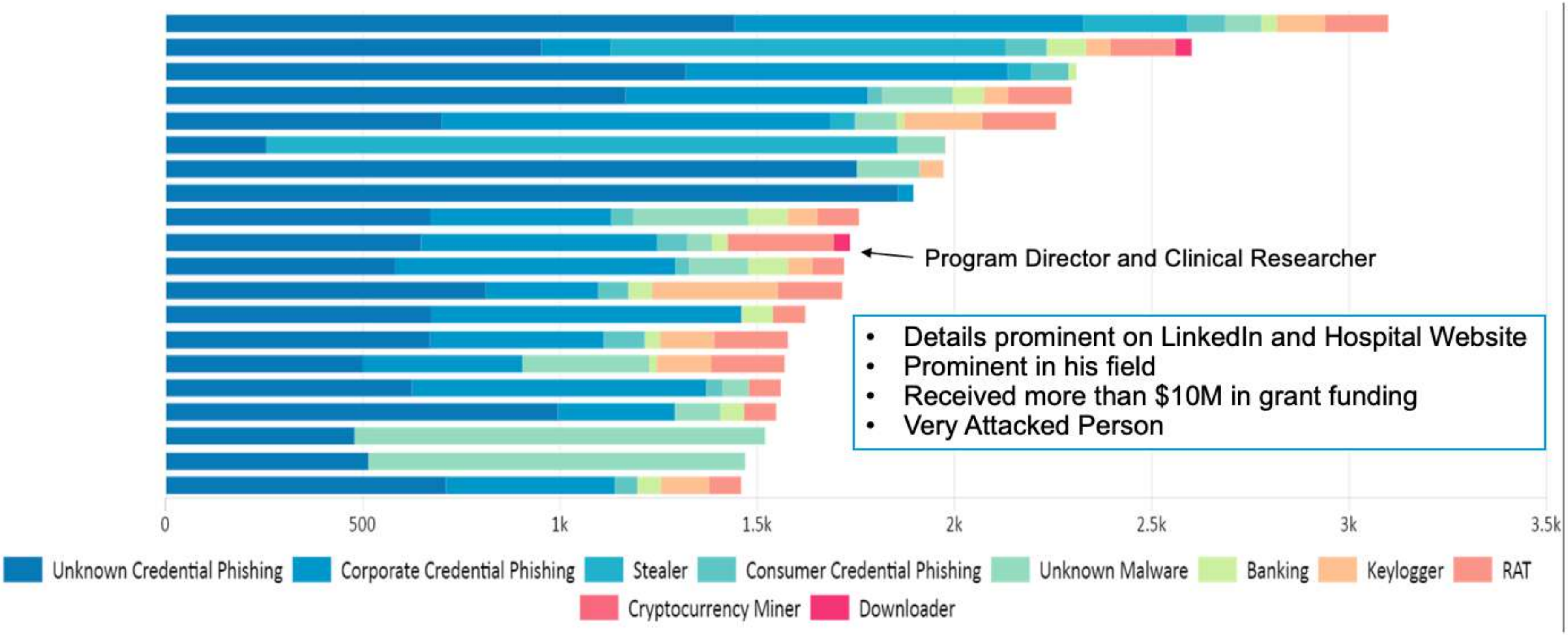
Threat Actors Shift around Security Measures



How to address Business Email Compromise/Email Account Compromise



Attacker's View – Teaching Hospital



Program Director and Clinical Researcher

- Details prominent on LinkedIn and Hospital Website
- Prominent in his field
- Received more than $10M in grant funding
- Very Attacked Person

proofpoint.

Speaker

Sue Bergamo, CIO & CISO, Episerver

Sue is the CIO & CISO of Episerver, a global digital Commerce company. As an executive, she brings her leadership and broad technology experience to help companies concentrate on growth by promoting innovation and productivity enhancements through application development, infrastructure operations, data analytics, business process optimization and talent management.

Sue is a Board member for SIM (Society for Information Management), co-chairs the SIM Regional Leadership Forum (RLF) Mentorship Program and is a member of the CIO Roundtable.

In another professional interest, Sue is a technical and business advisor to several startup companies and is the Program Director for Brandeis Universities Masters in Security program.

What’s the disruption all about?

- One of the most trusted means of communication is email. Yet, an unsuspecting user is vulnerable to many types of cyber attacks. We’ve all heard these terms – spam, phishing, ransomware, spoofing, impersonation, malware.

- For businesses, these attacks can mean countless hours of replacing devices, understanding where lost data has traveled, losing revenue, loss of brand reputation and customer trust. When a company has become the victim of a ransomware scheme, they can end up paying large fees to cyber criminals and still may not ever get back their data.

- No person or company is unsusceptible to the fraud and criminal intent of these unscrupulous thugs. Though many non-profits and small businesses are frequently targeted. Senior citizens are often the focus of malicious campaigns and identity theft is one area where these criminals love to obtain privileged data. Account compromises can be disastrous for any firm or household and no one can be to careful.

- Many of the individuals involved in these campaigns, come from foreign countries and failed nation states. These individuals are typically below the poverty level and are paid wages that feed their families. All they have to do is trick as many people as they can to fall for their schemes. While many of us may consider these individuals criminals (and they are), many are just trying to stay alive and are victims themselves.

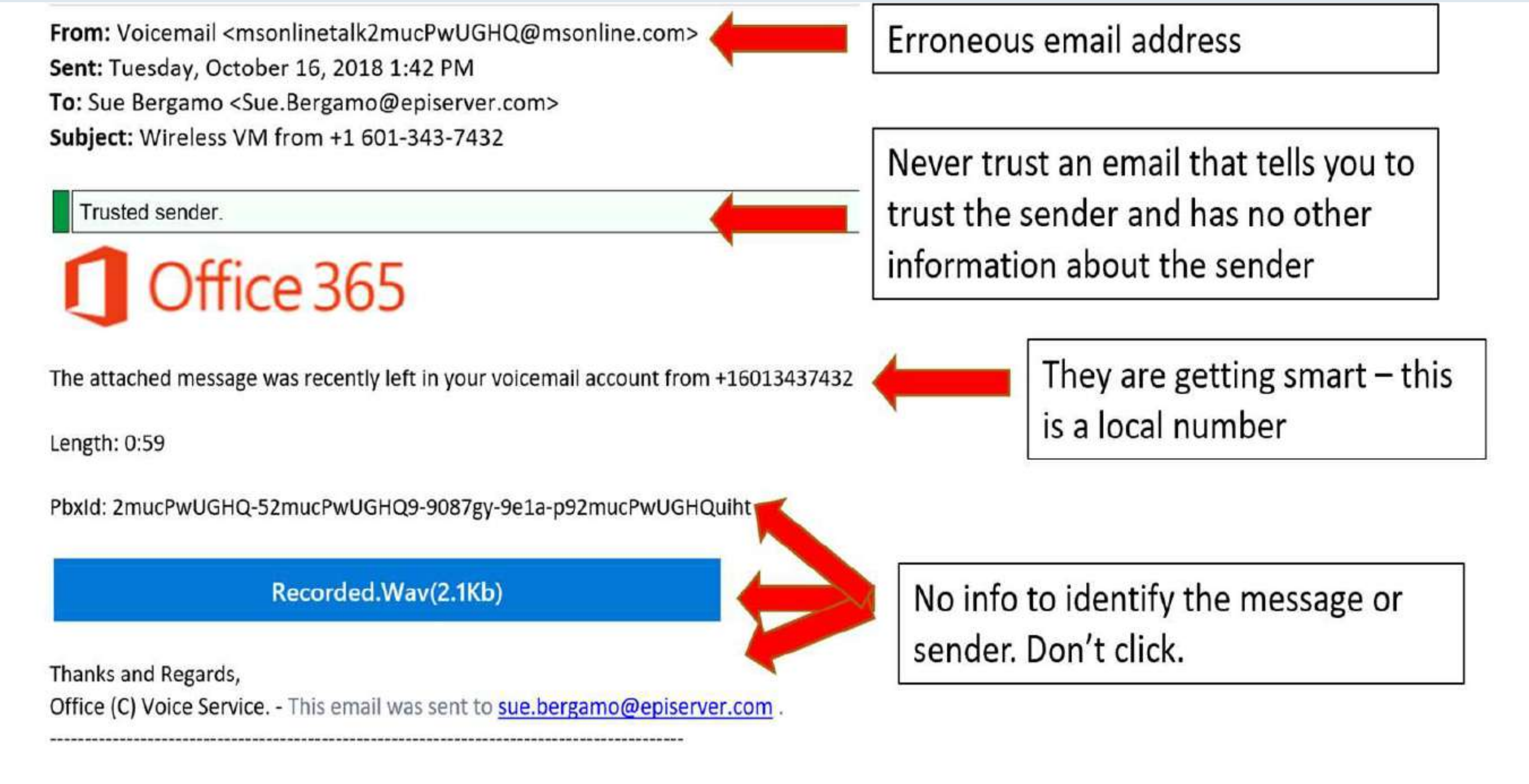
So how can you defend against these perpetrators?

There are all sorts of technologies that can be used against email security schemes, but the best defense is education. At my company, we have an annual security program that continues to teach our employees to be aware of their sensitive data and how to protect it from theft.

Some of the techniques that hackers use to attempt to fool people into their scams:

- Impersonating superiors, heads-of-company or other authority figures. These individuals may be very well informed about you, your role and the company.
- Any request for bank information, accounts or to send money to another address.
- Email scams typically contain misspellings and improper grammar (a give-away that the communication is false).
- Hover over links to determine if they are real and lead to a legitimate site.
- Copy/paste links into a browser instead of clicking on them from within an email. Often, clicking a link will download a malware script and infect your device.
- Any message that states it’s time sensitive or urgent should be considered suspicious.
- Within a browser session, be careful of clicking on an advertisement, as many contain malware downloads.

Example 1



From: Voicemail <msonlinetalk2mucPwUGHQ@msonline.com>
Sent: Tuesday, October 16, 2018 1:42 PM
To: Sue Bergamo <Sue.Bergamo@episerver.com>
Subject: Wireless VM from +1 601-343-7432

Trusted sender.

The attached message was recently left in your voicemail account from +16013437432

Length: 0:59

PbxId: 2mucPwUGHQ-52mucPwUGHQ9-9087gy-9e1a-p92mucPwUGHQuiht

Recorded.Wav(2.1Kb)

Thanks and Regards,
Office (C) Voice Service. - This email was sent to sue.bergamo@episerver.com .

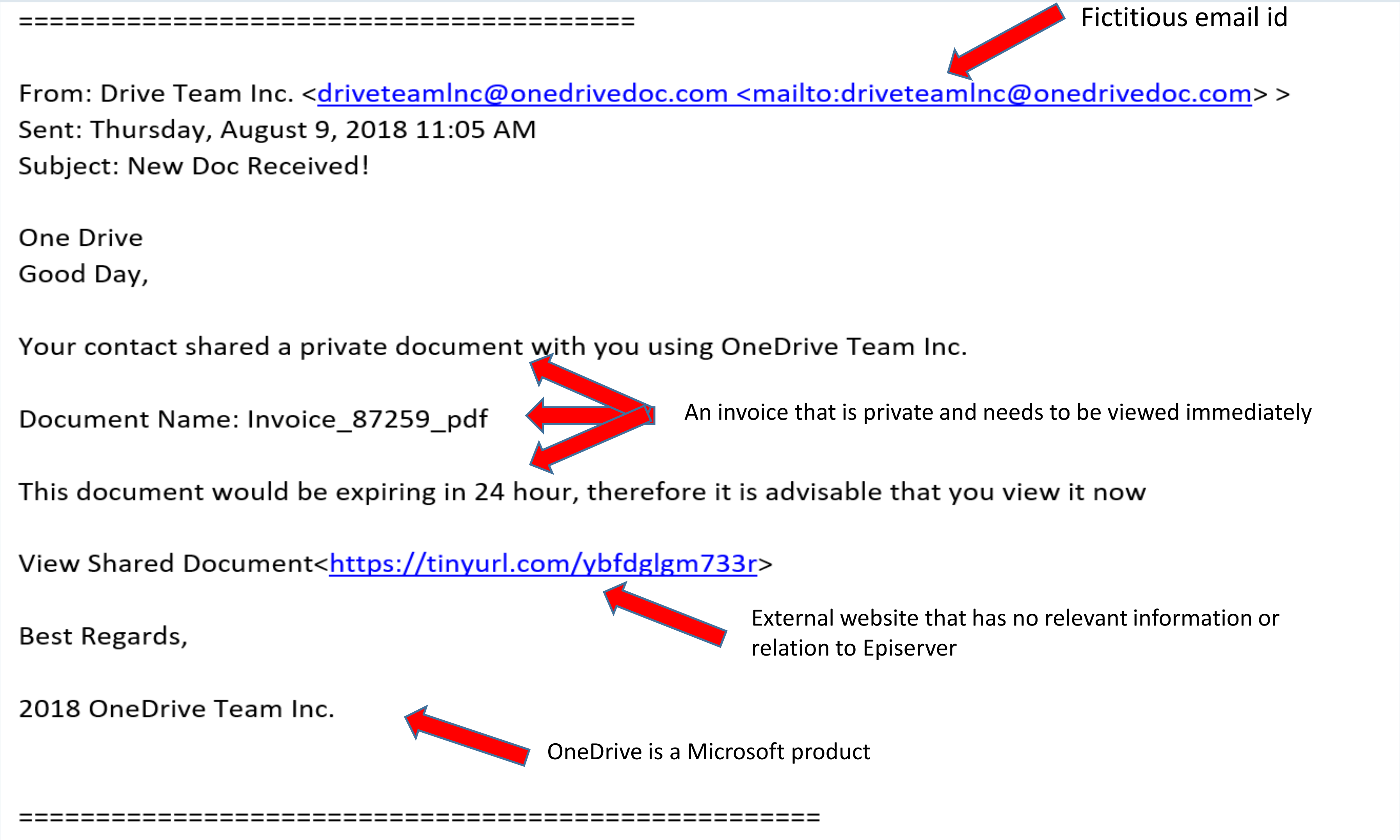
Erroneous email address

Never trust an email that tells you to trust the sender and has no other information about the sender

They are getting smart – this is a local number

No info to identify the message or sender. Don't click.

Example 2



==

From: Drive Team Inc. <driveteamlnc@onedrivedoc.com <mailto:driveteamlnc@onedrivedoc.com> >
Sent: Thursday, August 9, 2018 11:05 AM
Subject: New Doc Received!

One Drive
Good Day,

Your contact shared a private document with you using OneDrive Team Inc.

Document Name: Invoice_87259_pdf

This document would be expiring in 24 hour, therefore it is advisable that you view it now

View Shared Document<https://tinyurl.com/ybfdglgm733r>

Best Regards,

2018 OneDrive Team Inc.

===

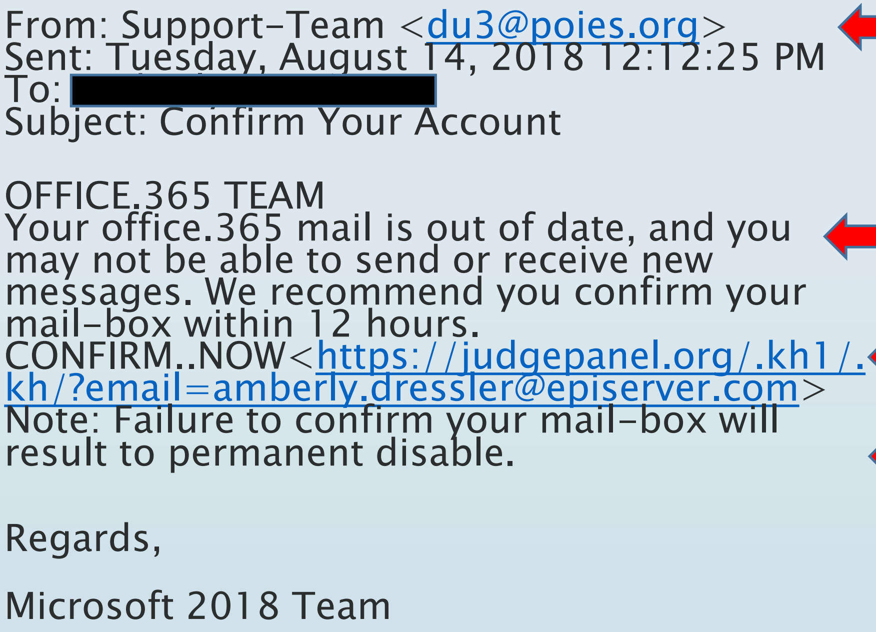
Fictitious email id

An invoice that is private and needs to be viewed immediately

External website that has no relevant information or relation to Episerver

OneDrive is a Microsoft product

Example 3



From: Support-Team <du3@poies.org>
Sent: Tuesday, August 14, 2018 12:12:25 PM
To: [redacted]
Subject: Confirm Your Account

OFFICE.365 TEAM
Your office.365 mail is out of date, and you may not be able to send or receive new messages. We recommend you confirm your mail-box within 12 hours.
CONFIRM..NOW<https://judgepanel.org/.kh1/.kh/?email=amberly.dressler@episerver.com>
Note: Failure to confirm your mail-box will result to permanent disable.

Regards,

Microsoft 2018 Team

Fictitious email id

An urgent request that must be taken care of immediately

Requests sign-on credentials

Episerver IT wouldn't permanently disable the account

Microsoft wouldn't contact you

Putting technology to work

➢ Starting with the user's device:

- Use anti-virus software to protect against downloaded files with malicious content
- Keep OS patches up to date
- Use device encryption techniques to further protect data
- In O365 – protect sensitive emails by sending via confidential, encrypted or do not forward (Options)

➢ At the network level:

- Firewalls should be kept up to date with new signatures, patterns and security patches
- Do not use open IP ports
- Further protect users by using group policies (access control)
- HTTPS vs HTTP (secure transmissions)

➢ As a Consumer:

- Use VPN on your phone and laptop for secure sessions
- Home Wi-Fi should be password protected
- Wi-Fi access that is Open = everyone can see your info (use VPN instead)
- Never enter your credit card information into a site that doesn't have lock symbol or state that it is secure

ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?