

Combating Business Email Compromise & Email Account Compromise

February 19, 2020



Combating Business Email Compromise & Email Account Compromise



Today's web conference is generously sponsored by:

proofpoint.

https://www.proofpoint.com/

Combating Business Email Compromise & Email Account Compromise





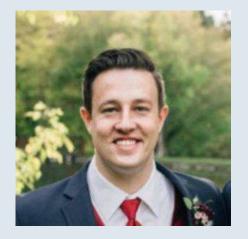
Moderator

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



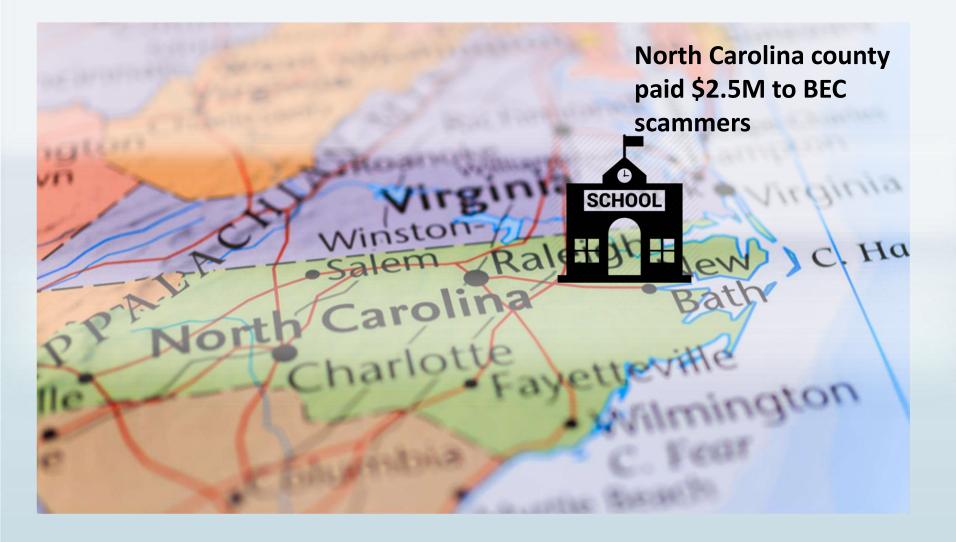


Speaker

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.







Connors snaps women's soc Lady Johnnies bead into Big East play out Xau BEC Scam Costs Media Giant Nikkei \$29M

> BEC Fraudsters Divert \$742,000 from Ocala City •

Governmen

TRUE

fac: (5GI) (()

GHAM

ev in Actuaria)

the second all must

Still Vice President Caroline Zottl said in an second.

coster of catoper-organizations through schet to staffed the Power to ire/Klegartor workers, which is run by the SOI Orgainstions Committee cach year. Potential equivisations apply to the consession, which reconstrands visible organizations to the SGI floor. Hour members then

Texas School District Loses 2.3M in BEC Scam

an organization, the Relientic Society has

organized Drug Information Association

airro to collector assignment of oppor-

atteng wadents

tanifies in the pharmaceutical andristry

Sould: The pre-dental chin events to more

evaluation of opportunities in the field.

of devial medicing and provide visidents

with the sesaurces to successfully apply

ner clourly with international non-profit

Operation Smile, which weeks with an

as dontial school. The group plane to par

The Pre-Dental ClabyOperation

Cruit Automation Association, Also

votes for each organization were then tions are listed and described below averaged to determine the final carA rig. Budgetary oning groups were the

macrow, it has now been revised,

Old recognition allows appleted earl

n campus. Official organizations

whiley for reserve

operativity disabled madents. V ach p of buddlers specide quality sure trajeffect out Chair previates study

leadin' this

and also postocipates at group events

description Society of Containers

Pharmerists a professional organism-

tions for corrections phanesis in that alread

as rated awareness among madents of

opportunities in the field of consulting

decidency of Managed Cure Pharma

come part of a larger organization, the Sr. John's chapter of AMCP will provide

networking opportunities for students in-

Cross Club will del m a branch of the

national Red Cipus and purvide and and

August Par, a pharmaceutical org

And Cross Chain the St. John's Bard

spusied in managed cars phermacy

volument any ices to these in need.

Town of Erie Paid \$1M to BEC Scammers

more welly served

a abere and the li-

where wants wrethers

in that when speed a thir annuar chara us ordered his they can do suspending "Jush day how you be done on pres-

tern right them." "But also were as make the deasts offices

mante with contra "Cos of the first things I did, which

ALC: N

actuals how a g hrian i a rich And alter the bysch hard any

FEDER 0



\$26.2B+

Direct losses worldwide

David Third/Nex. ni Pai, LIVE

The 13 approved groups will join the organizations strendy neorginized by Two groups, the Actuarial Club and previously as organization, the newly re-

"stille K Interventional, were previously ocountand organizations that have new ed to the budgetary consists. Deux Information: Association was

New groups are added to the official also previously a campas group, his betest not officially recognized since 2004.



will parter disept that représente-De lan Fache ration des ach moving and or regard which and other bit in

or the providence financial state only

- Fred 22 hills

· this Wat



but not officially recognized since 2008. Stil recognition allows appleut-exit sups the ability to reserve meeting

Sould: The pre-dental chin courts to more avaivation of opportunities in the field. of devial medicing and provide vaulents with the bestrance to successfully apply in donial school. The group plane to part ner clourly with international non-profit Operation Smile, which weeks with an

opplication is the field of coordina Academy of Managed Care Pharma

cause part of a larger organization, the Sr. John's chapter of AMCP will provide networking opportunities for students insensed in managed cars pharmery. And Cons Chill the St. John's Red. ette dors ministeri tour merrineful with their love. "Dask checking ray be done on page. sample devan" Dam said. "Ten sain stir man willy served. dynamical more approaches this, they will be manage which seems

Har

"I harrially work he doe made

Main

New groups are added to the official noster of campus organizations through whet in stalled the Power to (re)Organize process, which is run by the SGI Orgacivations Committee cach year. Potential organizations apply to the controller, which reconstands visible organizations to the SGI floor Floor members then

6M

have a g have any

Associated to Business Email Compromise in 2019 alone

FBI

It is a matter that everyone at entit supports is that people on. They sary int is a week. Anal some wooded his here about its a least way? And and e decide to hide their ses-



Cattle & International, were previously recognized organizations that have now ed to the budgetury consists-Drug Information Association was also previously a company group, but became macrous it has now been revised.

on campus. Official organizations

gars to collivate avogeness of opportanifies in the pharmaceutical industry attong wadents The Pre-Dental ClabyOperation

Cross Club will del m a branch of the national Red Circs and percede aid and volunted netvices to these in need. Kappat Par, a pharmaceutical org

of aberr and the liable or po to the marks and thack out an oren right them." "His also warm as make the deasts offices and women anothers "One of the first things I that which

h looking too the Back Placer

On

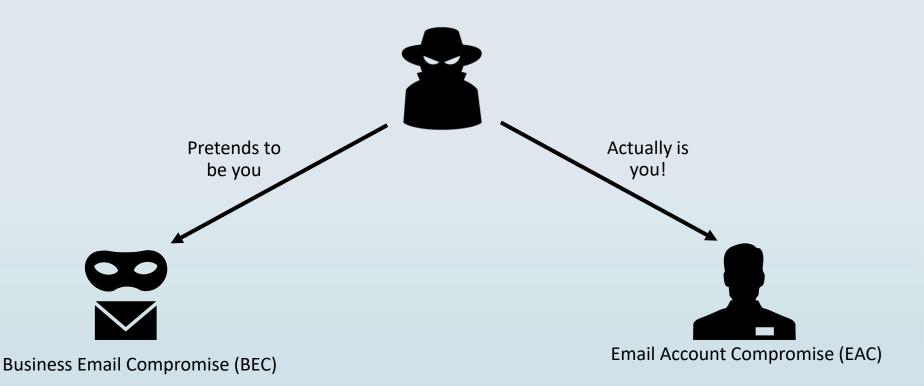
Hich

\$1.7B

for mader for lat 2 weather houses are house a

Email Fraud Leads to Two Main Threats

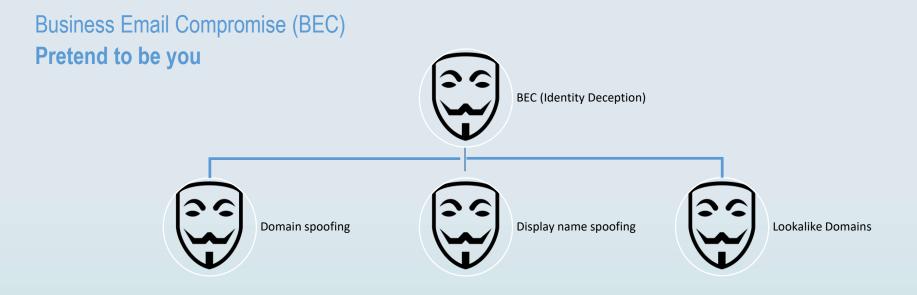




8

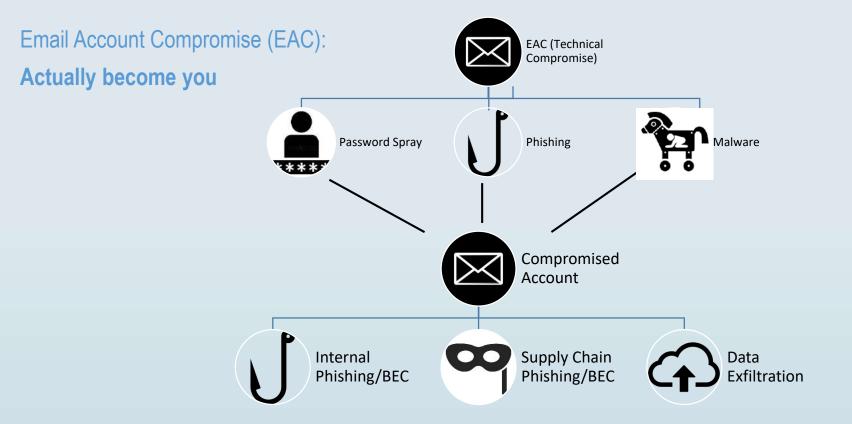






What's BEC/EAC?





Threat Actors Shift around Security Measures







Personal Webmail



Cloud Apps



Web



Supply chain





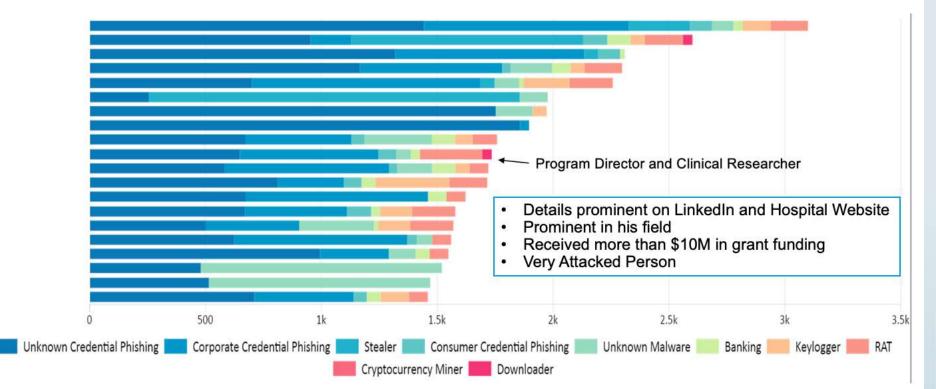
How to address Business Email Compromise/Email Account Compromise





Attacker's View – Teaching Hospital





proofpoint.

Combating Business Email Compromise & Email Account Compromise





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









Fictitious email id

From: Drive Team Inc. <<u>driveteamInc@onedrivedoc.com <mailto:driveteamInc@onedrivedoc.com</u>> > 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



An invoice that is private and needs to be viewed immediately

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

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

Best Regards,

External website that has no relevant information or relation to Episerver

2018 OneDrive Team Inc.



OneDrive is a Microsoft product

ISSA IIILEIIIALIUIIA

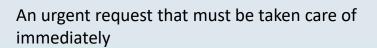
Example 3

From: Support-Team <<u>du3@poies.org</u>> Sent: Tuesday, August 14, 2018 12:12:25 PM To: _______ 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<<u>https://judgepanel.org/.kh1/.</u> <u>kh/?email=amberly.dressler@episerver.com</u>> Note: Failure to confirm your mail-box will result to permanent disable.

Regards,

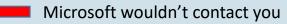
Microsoft 2018 Team



Requests sign-on credentials

Fictitious email id

Episerver IT wouldn't permanently disable the account





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



www.issa.org

QUESTIONS?