Phishing-Proof Your Staff and Software Systems

Presenter:

Joe Basirico

SVP of Engineering at Security Innovation

CONEXXUS

solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 15 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: **info@conexxus.org**

CONEXXUS
solve forward

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Moderator

Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speakers

Joe Basirico
Security Innovation
jbasirico@securityinnovation.com

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS
solve forward

2019 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
August 8, 2019	Application Security 101	Denis Sheridan	Synopsys
August 29, 2019	Phishing-Proof Your Staff and IT Systems	Joe Basirico	Security Innovation
September 2019	Updated Data Science Presentation	Ashwin Swamy Thomas Duncan	Omega ATC Omega ATC
October 2019	Easy PCI—How to Make PCI & Attestation Easier	Ajith Edakandi	Hughes
November 2019	Outdoor EMV	Brian Russell Linda Toth	Verifone Conexxus
December 2019	TBD	Sam Pfanstiel	ControlScan

CONEXXUS
solve forward

NACS Show
October 1-4, 2019
Atlanta, GA

TECHEDGE

In partnership with CONEXXUS

Booth # 3755

Conexxus thanks our 2019 Annual Diamond Sponsors!

mSHIFT. Relevant. Mobile. Solutions.

Stuzo

Diebold Nixdorf

wex

HUGHES An EchoStar Company

GILBARCO VEEDER-ROOT

Cybera

SECURITY INNOVATION

CONEXXUS solve forward

Agenda

- Evolution of phishing attacks
- Hardening Staff & Software Systems
- Policies and incidence response

Phishing-Proof Your Staff and Software Systems

Presenter:

Joe Basirico

SVP of Engineering at Security Innovation

CONEXXUS

solve forward

EVOLUTION OF PHISHING ATTACKS

Phishing: Oldie But Goodie

- Email is an attack vector in 96% of incidents with social actions*
- Plethora of personal and professional info on web and social networks is making it easy
- Education is helping but unrealistic panacea
  - 4% of people will fall for any given phish*
- Anti-virus is helping but sophisticated techniques circumvent it
- Email technology is good at detecting malware
  - not social engineering and credential theft

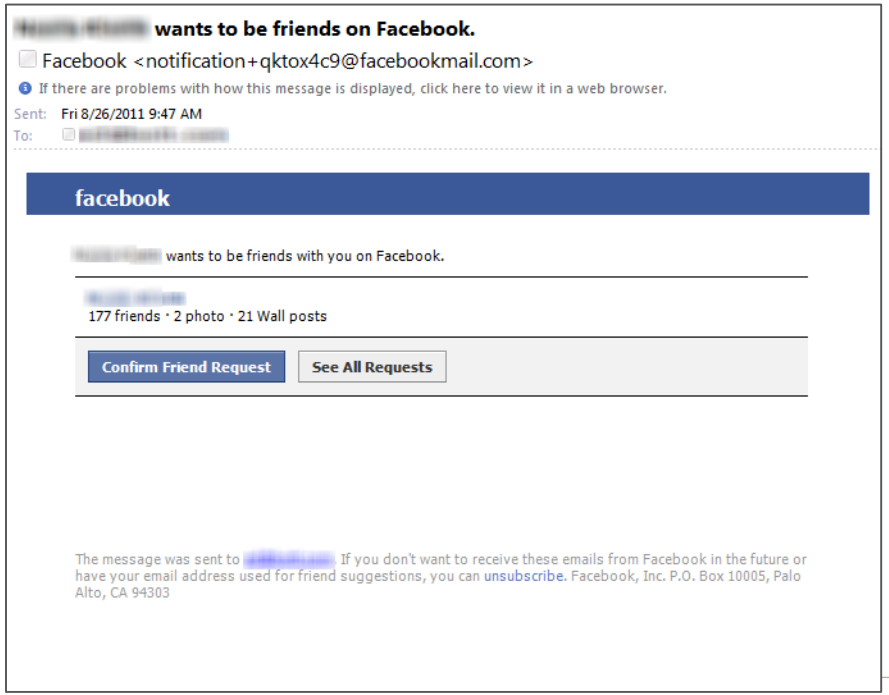
* Verizon 2018 Data Breach Investigations Report

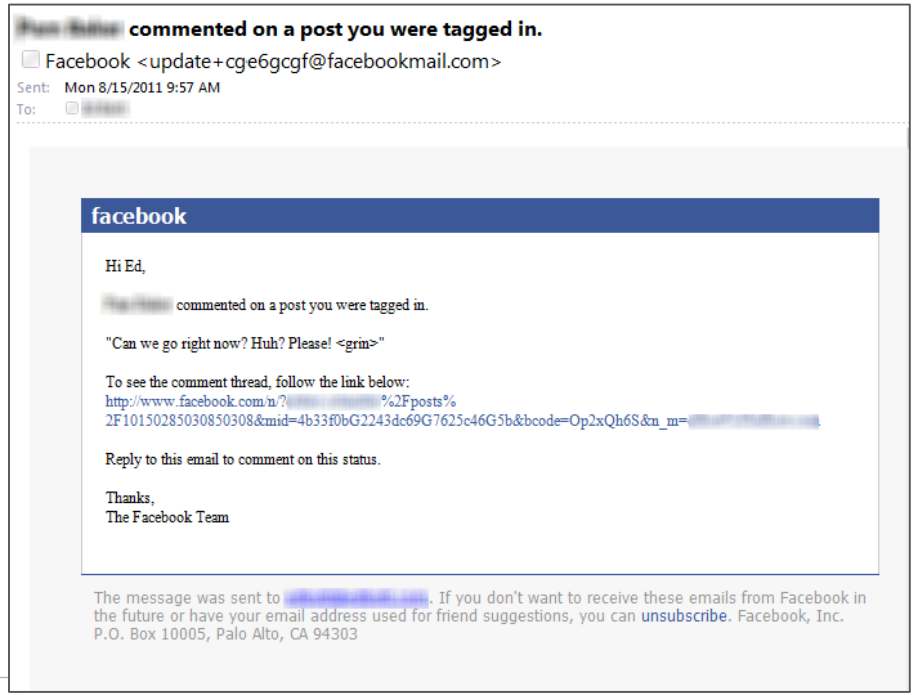
CONEXXUS
solve forward

Traditional Tactics

- Spear-Phishing, Pharming, SMiShing, Spy-Phishing, Vishing, Whaling, etc.
- Website Forgery/Tricks
  - Typo/Cyber Squatting: facebok.com, googlle.com, yahooo.com
  - Use of Sub Domains: www.xyzbank.user.com
  - Hidden/misspelled URLs - prominent on social networks where trust is often assumed
  - IDN Homograph Attacks (similar looking characters)
  - bitsquatting
- Pop-ups
  - Fraudulent messages that “pop up” for users when they are surfing the web
  - Hackers inject otherwise legitimate websites with code that causes pop-up messages to appear when users visit
    - Look legit. Click → taken to malicious site and infected

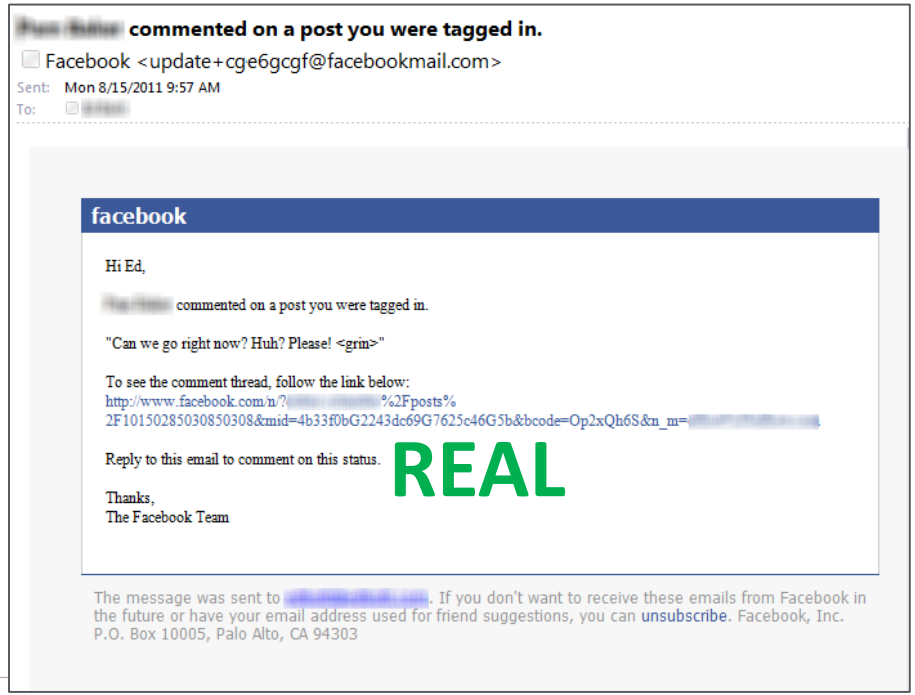
Real or Fake?





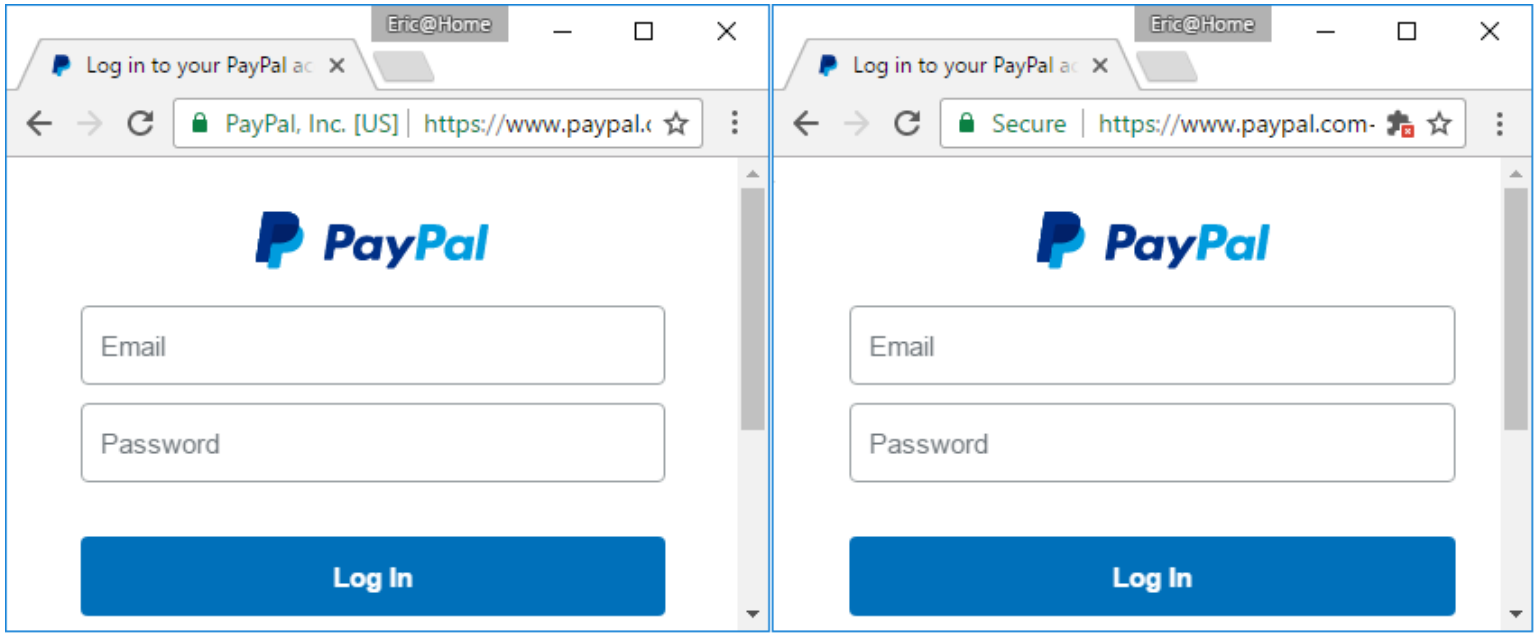
CONEXXUS
solve forward

Real or Fake?



CONEXXUS
solve forward

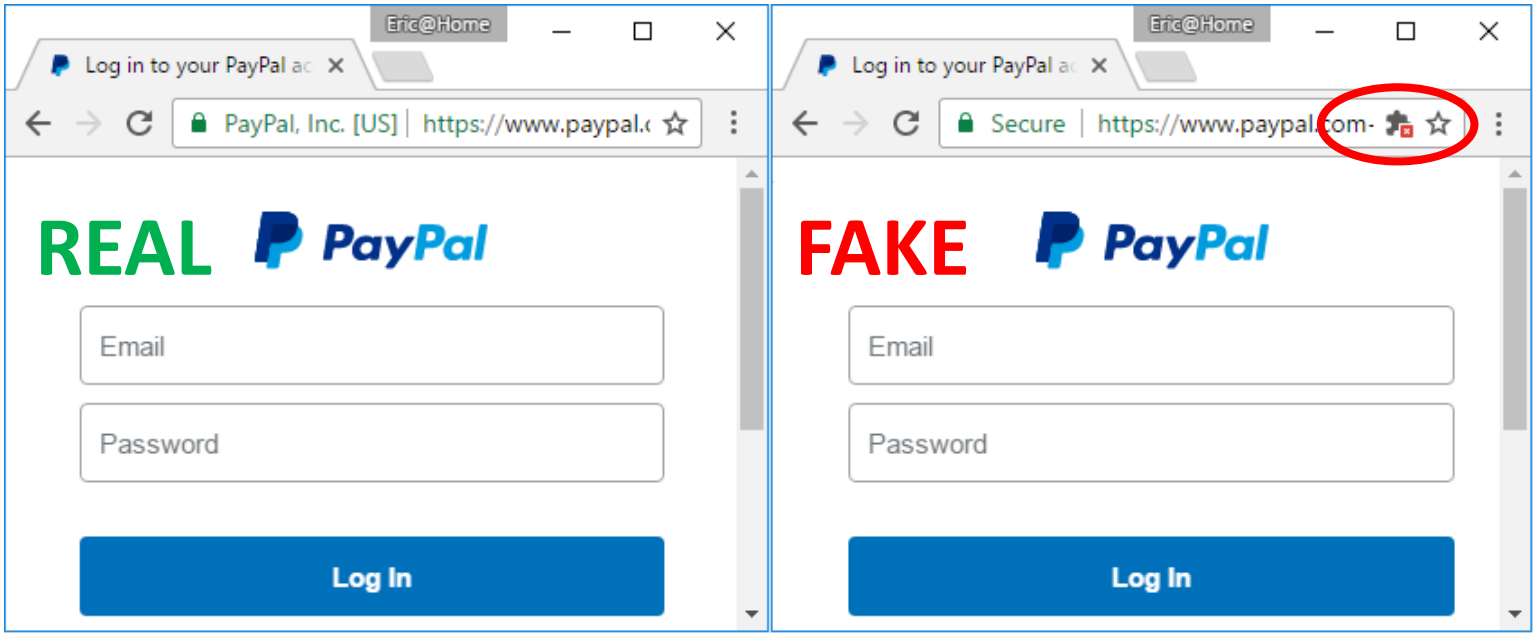
Landing pages look good!



One real, one fake, your account is at stake.

CONEXXUS
solve forward

Landing pages look good!



One real, one fake, your account is at stake.

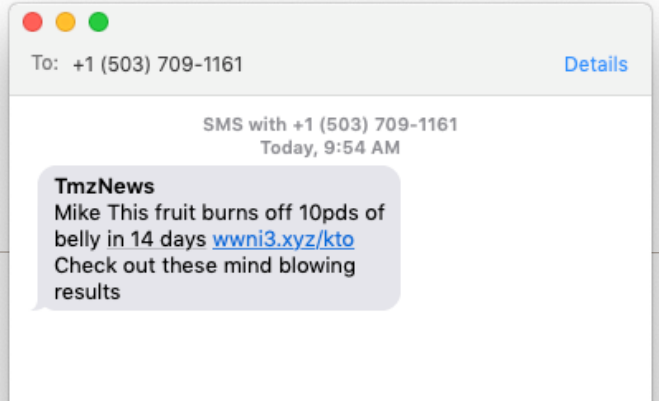
CONEXXUS
solve forward

Emerging Tactics

- e-Transfer alerts
  - Tricks people into thinking a transfer occurred; most want to investigate
  - Can target customers of many banks at once
- Stealth attacks
  - Blocks cloud service from seeing phishing page; shows only to target in real-time
- Social media scammers
  - Link to phishing resources, pay for advertising posts, enticing people to distribute content
- Big Company Scams/Skim
  - New Apple product released → number of fake websites imitating Apple services rose by ~1000%
  - Amex trick used base html element to hide malicious URL from antispam solutions

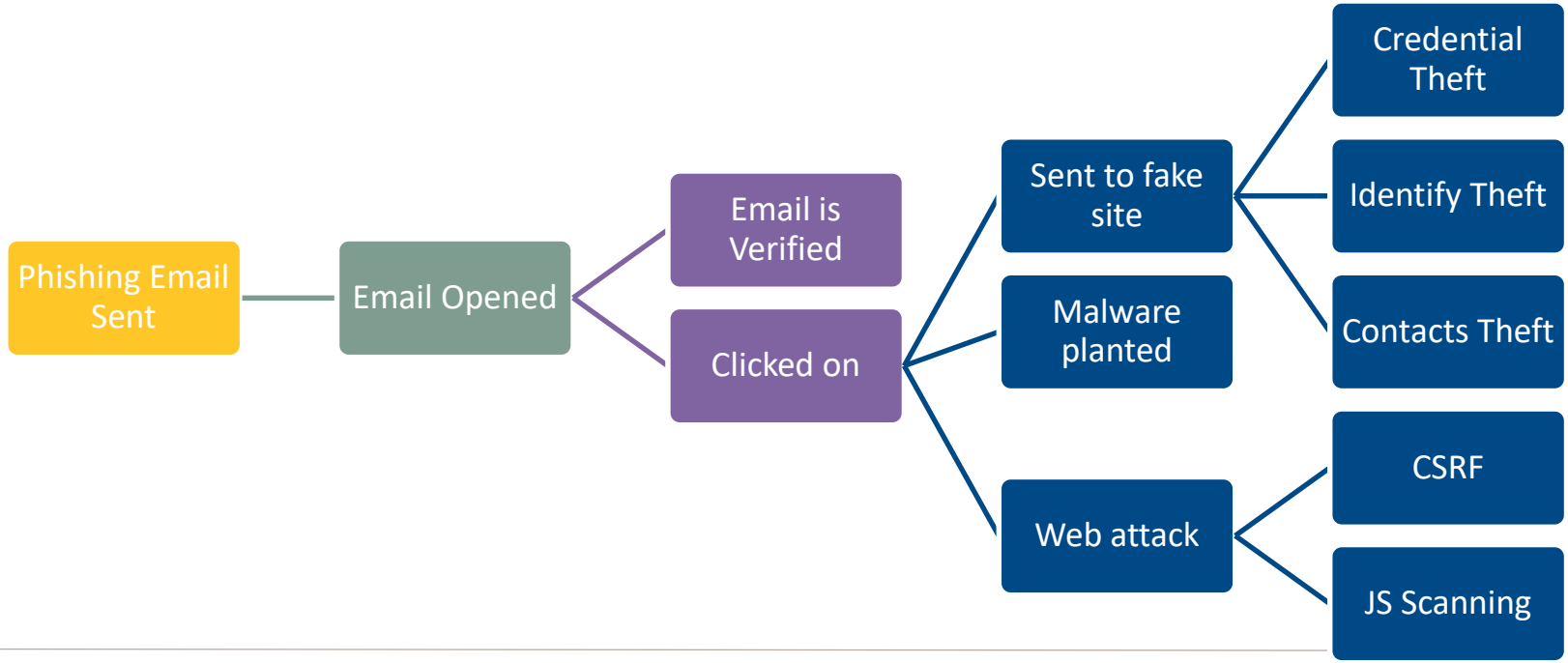
Mobile Phishing Attacks

- SMiShing” is similar to email-based phishing
- Mobile-specific phish kits attempt to mimic login screens of legit mobile apps
- Expanded attack vectors and ineffective controls make it dangerous
  - i.e. Link, TLS, authority, URL, spelling and grammar inspection
- Use mobile sensitive URLs



CONEXXUS
solve forward

Anatomy of a Phishing Attack



Impact for Petro

- Phishing is often a foot in the door to further attacks
- Don’t just think about the person being directly attacked, think about what they have access to.
- Train office and convenience store staff
- Back office PCs are often on the same internet connection as the PoS
- If you manage groups of stores it’s important to think about the whole network

HARDENING STAFF & SOFTWARE SYSTEMS

Defense In Depth

- Often, goal is to gain *initial* entry to network then expand
- For an attack to be successful, it must complete three steps:
  1. Email must make its way through the gateway to the user's inbox
  2. User must successfully execute the payload
  3. Payload must successfully communicate with external command/control server
- During each, there are defenses to thwart or minimize impact
  - ✓ Informed staff can serve as a human firewall
  - ✓ Reduced attack surface keeps doors to a minimum
  - ✓ Mitigating controls can prevent, delay and detect

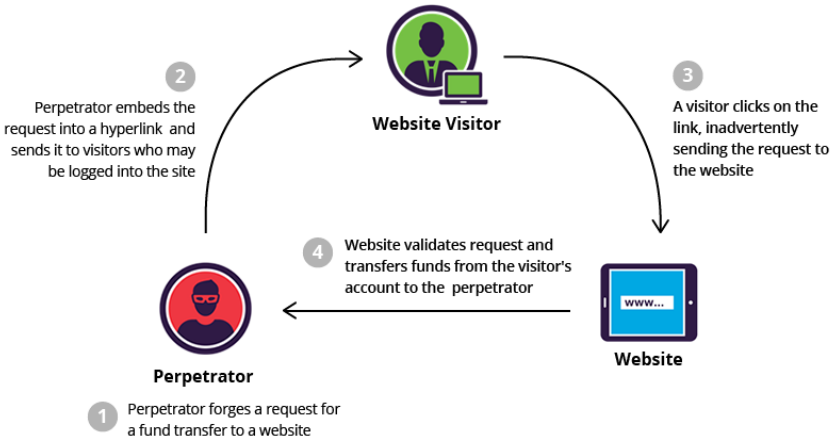
*2018 Verizon Data Breach

Making Phishing Easier

- Use Bad Software
  - Vulnerable to Web-based attacks
  - Exploiting poor design, attacker can take over a user's session, redirect user, and launch malicious popups
  - Evolution of rich client web apps, SPAs, HTML5, etc.
- Don't Patch Systems
  - Unpatched systems easy target for exploit
  - Malware implantation
- Assume your staff will make good choices
  - Attack techniques change quickly; most "training" is annual
  - Even the most informed will fall victim at some point

Cross Site Request Forgery (CSRF)

- Performs an unauthorized action on behalf of a user already logged into a Web site



CSRF Controls

- Enable Anti-CSRF tokens or controls
- Add “are you sure?” confirmation pages
- Use multi-factor authentication (out of band)
- If a request has expired credentials
  - After log-in, return to a safe state
  - Do not execute the transaction

Open/Unvalidated Redirects

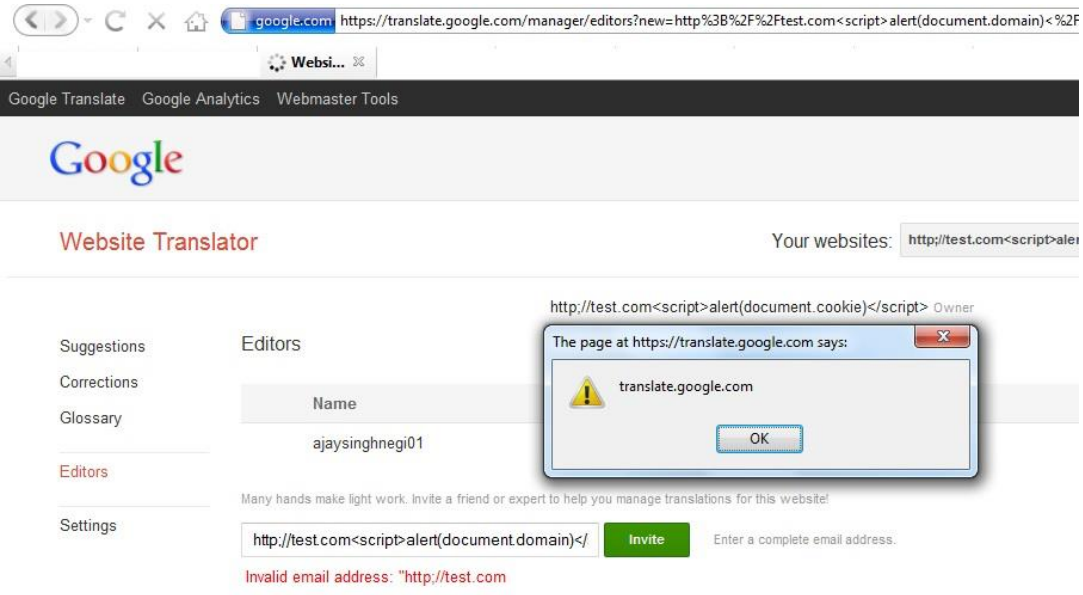
- Without proper validation:
  - Redirections can be manipulated, to a phishing site
  - Forwards can be used to bypass access control

- Attacker creates legitimate-looking URLs and login page, tempting users to enter credentials
- If attacker gets admin access, they may gain full control of the application
  - Very dangerous with cloud-based business apps like Office365
  - What could someone do with your CFO's Outlook login creds?

Mitigating Insecure Redirects & Forwards

- Review the code for all uses of redirect or forward
- Spider the site to see if it generates any redirects (HTTP response codes 300-307, typically 302)
- Identify all sources of input
  - Assume all input is malicious
  - Use an “accept known good” input validation strategy
  - Don’t assume some inputs (cookies, hidden fields) can’t be modified
- Use a Web Application Firewall (WAF) configured to flag/block redirects
- Be careful with destination parameters

Cross Site Scripting (XSS)



- Most web apps have this problem
- Carried out on a trusted website
- Occurs when raw data from attacker is sent to an innocent user's browser
  - Stored in database
  - Reflected from web input
  - Sent directly to client
- Typical Impact
  - Steal user's session or sensitive data
  - Rewrite web page
  - Redirect to phishing or malware site
- More severe impact
  - Attacker can direct all user's behavior and force user to other sites

CONEXXUS
solve forward

Mitigating XSS

- Validate user-submitted input and escape user-submitted output
- Whitelist inputs, accepting only expected characters and use an encoder library
- Don’t ignore issues where input through HTTP could make its way to output
- Never store passwords as cookies
  - Or other sensitive data, e.g., item price, account number, etc.
- Use a Web Application Firewall (WAF)
  - Configured to block XSS attacks

Cybersecurity Fundamentals

- Regularly update your security definitions
- Keep your security products current (spam filters, antivirus, firewalls):
  - On gateways, servers, and endpoints
- Ensure laptops or other removable devices require your security solution to include built-in antispyware and client-side firewall
- Separate User and Admin accounts
  - If target is a system admin, any elevated access (even local admin on a single machine) makes credential theft and stealthy persistence easier
  - Restrict from accessing email and browsers

Ransomware

- Lots of ransomware attacks recently
  - Baltimore, Newark, Atlanta, Sarasota, UK's NHS
- Encrypts individual files, extorts payment
- Sometimes you can decrypt, but usually the files are irrecoverable
- General security practices should be followed to protect yourself
  - Offsite backups are key
  - Anti-malware
  - Updates

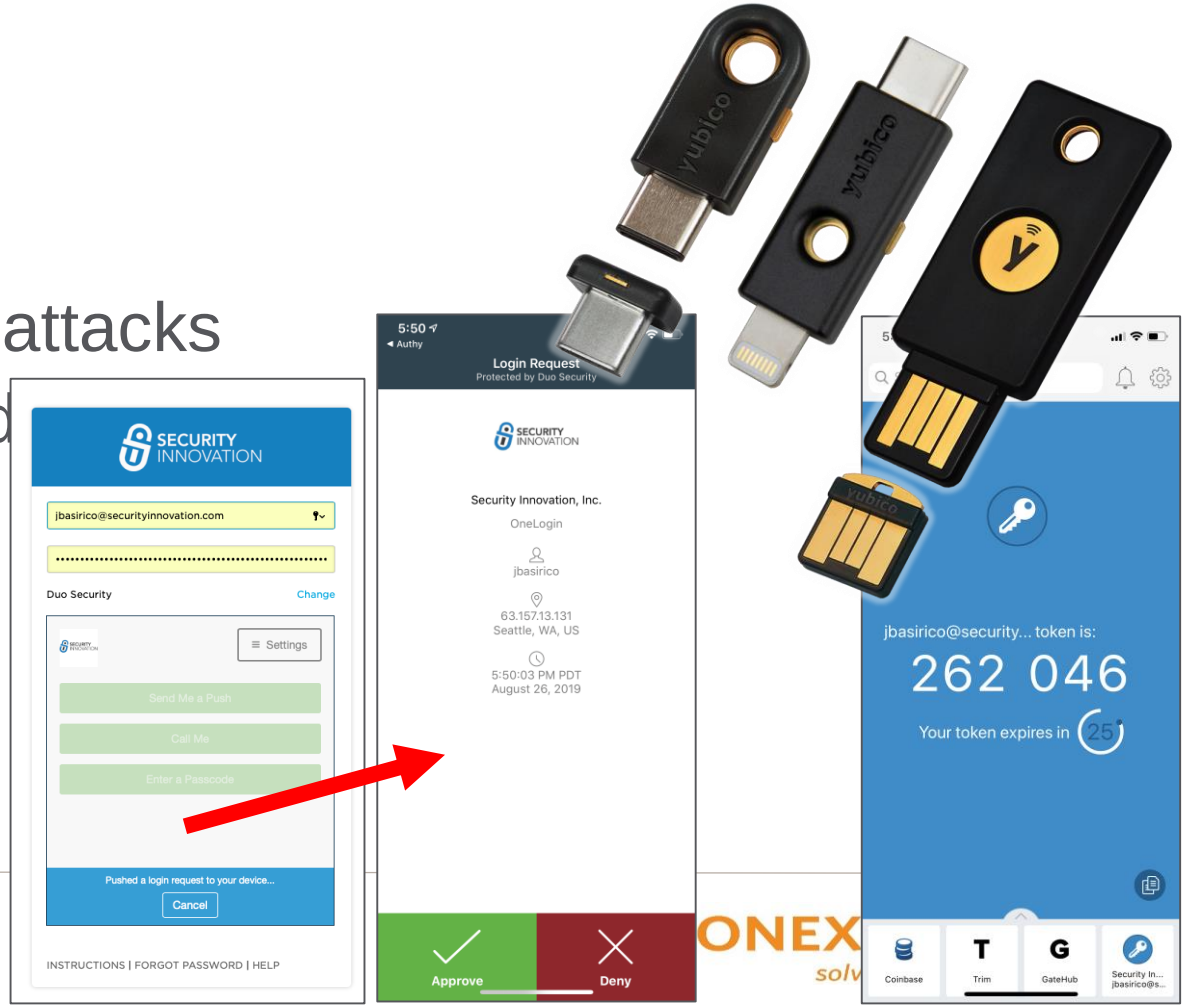
CONEXXUS solve forward

System Hardening Tips

- Minimize Attack Surface by…
  - Removing any unnecessary software
  - Disabling unnecessary services
  - Closing unused ports
  - Remove all default credentials
- Implement Network Segmentation
  - Identify critical assets and establishing access controls for each
  - Separate users into controlled network segments, physically or virtually
- Advanced hardening might involve:
  - Installing only bare necessities for required functioning, e.g. file and print sharing
  - Require complex passwords and MFA
  - Set baseline of "normal" network behavior; monitor for anomalies

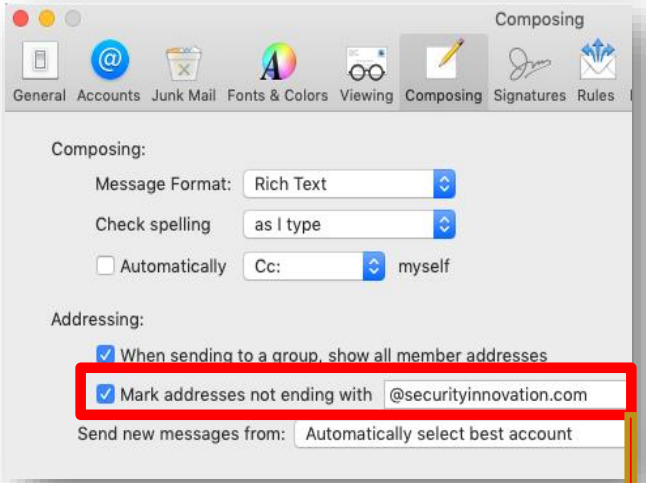
MFA/2FA

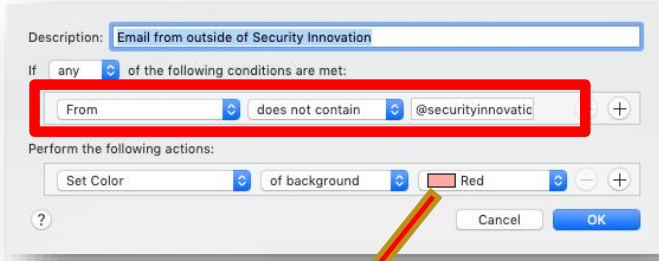
- Can stop many credential theft attacks
- Stop the spread of Phishing attacks
- Adaptive Authentication can also help

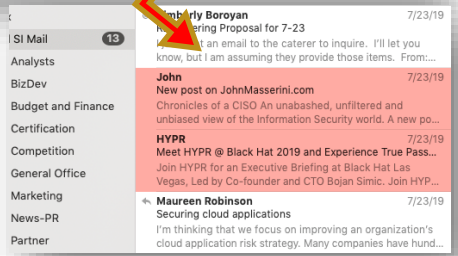


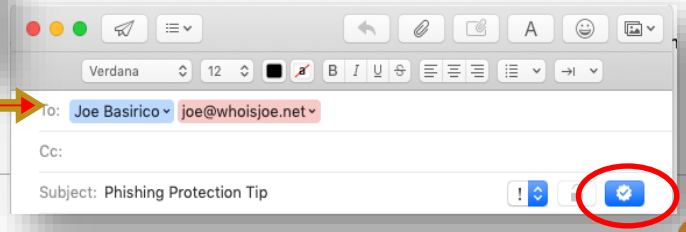
Leverage Email Client Settings

- Some mail clients allow you to mark any email to/from people outside of your organization
- Use digital signatures so recipient knows it's you sending the mail





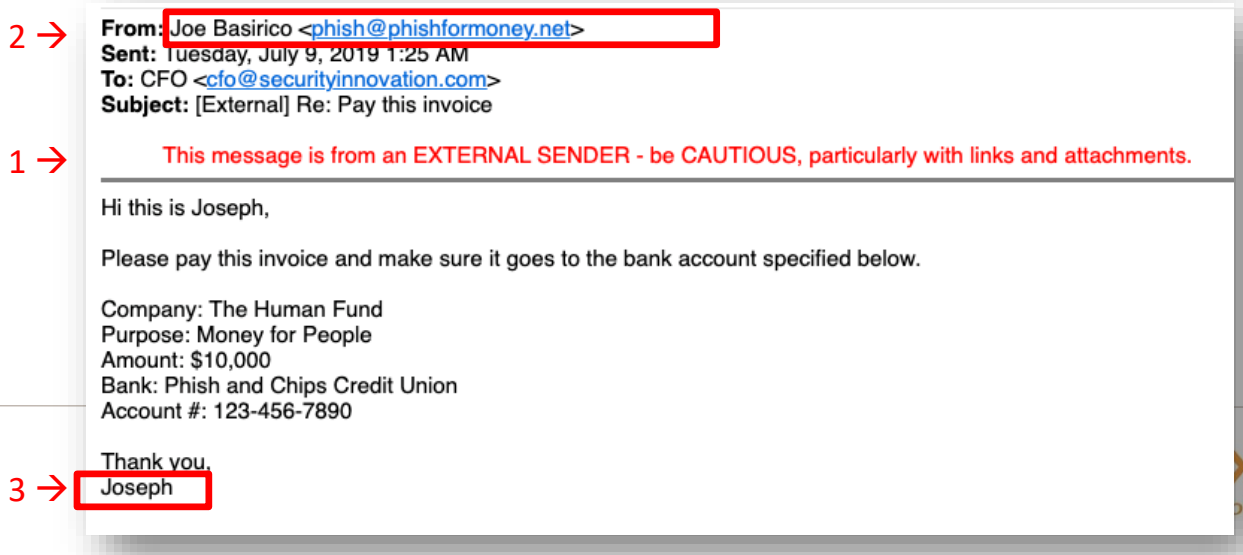




CONEXXUS
solve forward

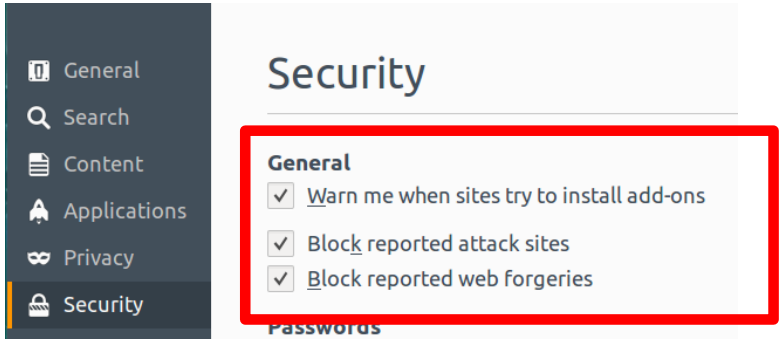
Use Email Server Settings and Guidelines

1. Auto-tag emails from outside your organization with a warning message
   … but also be observant:
2. Check the email address if the message looks a little suspicious
3. Think about how senders refer to themselves
4. Check for misspellings and grammar mistakes
5. Gut check, is this a reasonable request?
6. Double check in another channel

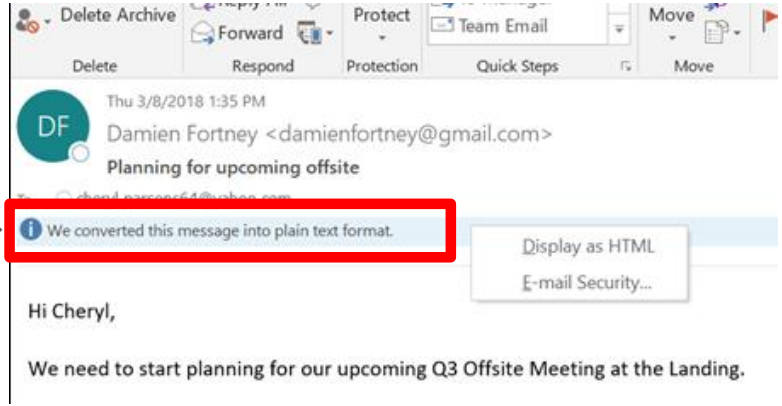


Properly Configure Web Browsers

- Train users on best practices, or have IT do it



Train users to look for this message →



CONEXXUS
solve forward

POLICIES & INCIDENCE RESPONSE

Policies

- Can be either be written or technical procedure, e.g.:
  - Software Restriction Policies to restrict common methods of executing scripting languages and prevent common initial payload execution methods
  - Limit access to critical devices and services by employing access control policies
  - Tighter financial controls can help prevent scams including wire transfer frauds
  - Social media activity can be regulated and monitored
- Ensure new hire and *regular* InfoSec training
  - Multi-modal, e.g., not just CBT
  - More than annual
  - Test for proficiency to avoid over-training
- Keep stay updated on latest phishing techniques, even if just written email

Incidence Response Plan

- A well-designed plan can mitigate the impact of attacks
- Don’t assume this is an isolated event
- Think about and document the following:
  - Detecting: what mechanisms will minimize breach duration
  - Analyzing: where have phishing attacks come from
  - Containing: who has been affected/targeted
  - Eradicating: education, tooling, more
  - Recovering: if a breach happens can you recover
- Post Incident Handling
  - What was compromised? Lessons Uncovered?
  - Policy changes. Configurations applied

Testing your Incidence Response
Tabletop Exercise

- Your organization was notified it may be targeted through spear phishing emails and social engineering phone calls
- Items to discuss
  - Do your end users know what to do with a suspicious email or phone call?
  - What does your policy say about reporting suspicious emails?
  - How do you notify end users? IT Staff?
  - At what point do you communicate the event to upper management?
  - What do you do if individuals click on link?
- Items to report
  - Did communications flow as expected?
  - Were processes and procedures followed?
  - Were there any surprises?
  - Was it triaged accordingly?

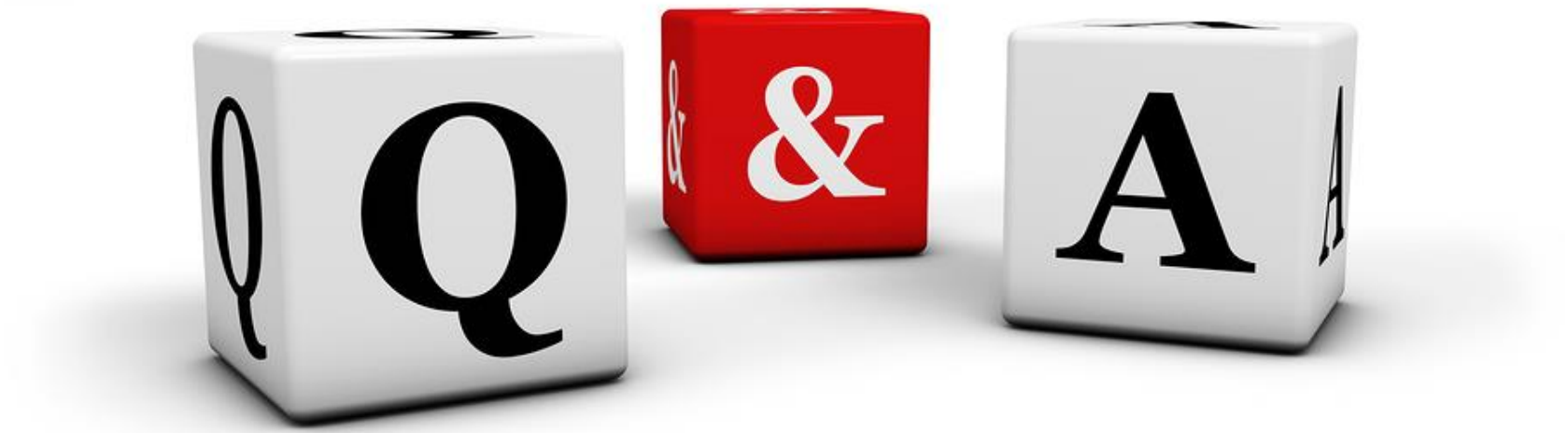
Final Thoughts

- Staff can be a great defense; treat them like other IT defenses
  - The are distributed across the network like sensors
  - They can act like firewalls, allowing or blocking attacks
  - They can detect attacks and raise alarms
  - They need “configuration and patching”
- Get staff involved in solution
  - Have them craft emails and test top ones organization wide
  - Reward users for reporting phishing attempts, even if successful
  - Offer prizes/recognition on technology, policy, or training changes that mitigate phishing
- Stay informed and relay to staff
  - Monitor phishing sites
  - Maintain knowledge on vulnerabilities, attacker techniques

THANK YOU!

Joe Basirico
jbasirico@securityinnovation.com
SVP of Engineering
Security Innovation

CONEXXUS
solve forward



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.