



Postal Customer Council® Workshop in a Box

Our Shared Responsibility:
Protecting the nation's mailing
ecosystem from evolving cyberthreats

Chris Nielsen
Deputy Chief Information Security Officer
U.S. Postal Service

February 4, 2021





Goal

Empower you with the knowledge, tools, and resources to further protect the nation's mailing ecosystem from cyberattacks

Agenda		
Topic	Slide	Time
My Bio	3	5 min.
2020 Cyber Successes at USPS	4 – 5	5 min.
The Mailing Ecosystem	6 – 8	5 min.
CISO and USPS Cybersecurity Strategy	9 – 14	5 min.
Phishing Attacks	15 – 20	10 min.
Resources	21 – 23	5 min.
Q&A	24	10 min.





Career Highlights

- In 2007, began federal career in law enforcement in the U.S. Postal Inspection Service's New York Division
- As a Postal Service Inspector, investigated financial crimes, mail fraud, child exploitation, and narcotics trafficking
- Prior to federal service, worked for SAIC, helping develop solutions on several information technology and cybersecurity projects, both domestic and in Europe
- Hold a Bachelor of Science degree in Computer Science from the William Paterson University in New Jersey
- Maintain ISACA certifications in Certified Information Security
 Manager, and Certified Risk and Information Systems Control



Chris Nielsen Deputy CISO





2020 Cyber Successes at USPS

Progress during an unprecedented year









Transitioned USPS workforce safely to telework

Secured the U.S. vote

Maintained cyber posture during record-breaking package volume delivery



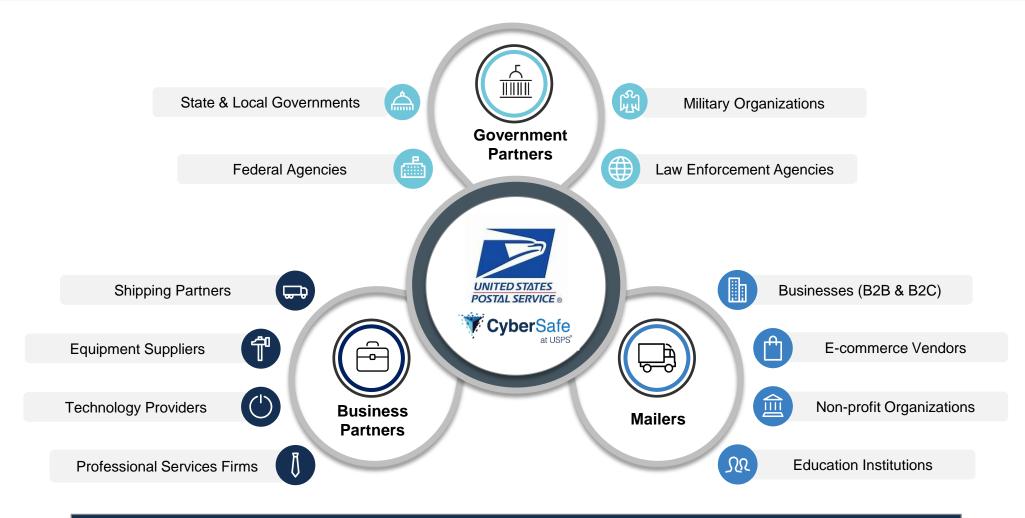


The Mailing Ecosystem

We're in this together



Securing Customer Experience Across the Mailing Ecosystem



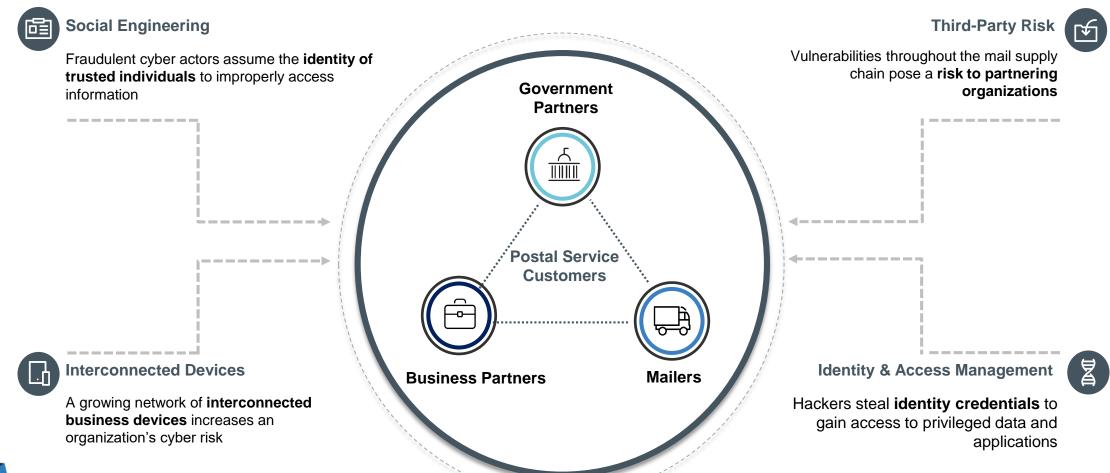
As members of a complex mailing ecosystem, it is vital that all mailing organizations, business partners, and government partners maintain secure and resilient IT networks.





Digital Disruptors in the Mailing Ecosystem

These disrupter create both threats and opportunities that will impact the security of the overall mailing ecosystem and create new business and shipping solutions for our customers.





CISO and USPS Cyber Strategy

Protecting the network that binds our nation



USPS Organizational Alignment



Postmaster General and Chief Executive Officer Louis DeJoy



Chief Information Officer and Executive Vice President Pritha Mehra



Vice President, Chief Information Security Officer Gregory Crabb



Deputy Chief Information Security Officer Christopher Nielsen



CIO

CISO





Vice President,
Chief Information Security Officer
Gregory Crabb









Manager,
Cybersecurity
Engineering
Douglas Glair



Manager,
Cybersecurity
Risk Management
William Jones



Manager,
Cybersecurity
Operations
Lynne Mitchell



Director,
Identity and Access
Management
Dorin Methfessel





CISO Strategic Objectives



Protect

Protect, **shield**, and **defend** the enterprise from cyber threats and prevent disruptive cyber incidents



Monitor the internal and external environments, detect attacks, and hunt for threat actors inside the environment



Respond

Respond to and **recover** from incidents, and **sustain** operations when incidents occur



Manage

Improve management, governance, compliance, education, and risk management



Innovate

Innovate to develop, deploy, and deliver new CyberSafe digital products and services





Cyber Defense by the Numbers



350+ CISO Staff



3.5M legitimate emails daily



100K+ malware messages blocked annually



970+ applications



~1.2M devices on network



~66,000 mail processing technology systems



551 business partner connections



151 countries connected



4,719 data transfer service connections





Global Cybersecurity Threat Landscape

2019: USPS was notified of a cyber incident attributed to "Ryuk" ransomware impacting USPS supplier Pitney Bowes preventing customer account

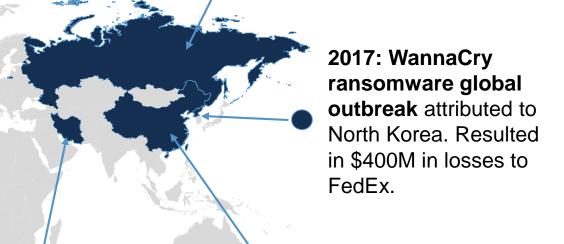
2017: 148 million PII records lost by Equifax due to a lack of a patch management program.

access.

ng
/

2013: Target's Point-of-Sale systems breached via HVAC monitoring system by cyber criminals seeking PCI data.

2020: Russia exploits SolarWinds to **infiltrate corporate and government networks worldwide.**



2018: Iranian hackers charged with **stealing intellectual property** from hundreds of U.S. universities and businesses.

2018: U.S. charged Chinese intelligence officers with attempts to steal aerospace technology intellectual property.





Phishing Attacks

How not to get hooked



Cyber Industry Stats and Risks to USPS

91%

of breaches start with an email¹ 50%

of cyber attacks are due to human error²

\$3.86M

is the average cost of a successful phishing attack for a company³

Risks to USPS



Impact mail delivery system

Damage physical and digital inventory

Loss of sensitive personal information

USPS reputational damage

A phishing attack against one member of the mailing ecosystem could impact the entire ecosystem



¹ wired.com ^{2,3} ibm.com



Watch for Emotional "Hooks"



Greed

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems too good to be true, it probably is.



Urgency

If an email provides a strict deadline for performance of an action, be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.



Curiosity

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.



Fear

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.





Examine These Items Closely



Email Signatures

A signature block that is overly generic or doesn't follow company protocols could indicated that something went wrong



Sender Address

If the address doesn't match the sender's name, be suspicious of the entire email.



Email Tone

We know how our coworkers and friends talk, so if an email sound strange, it's probably worth a second look.



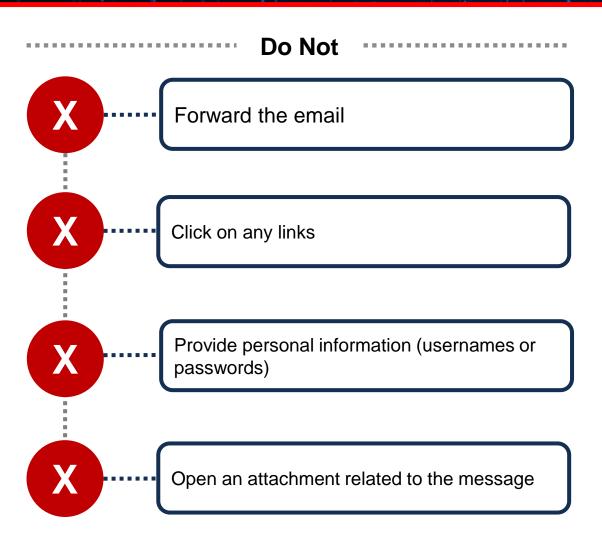














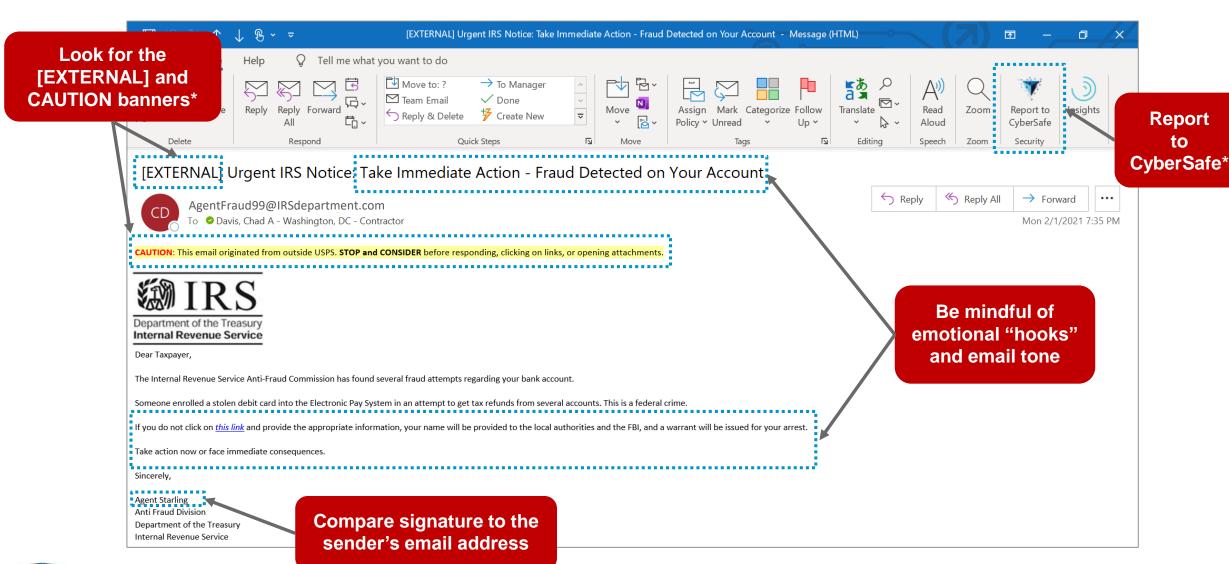


What processes does your organization have in place to respond to and report phishing attacks?





Example Phishing Email





* = specific to USPS

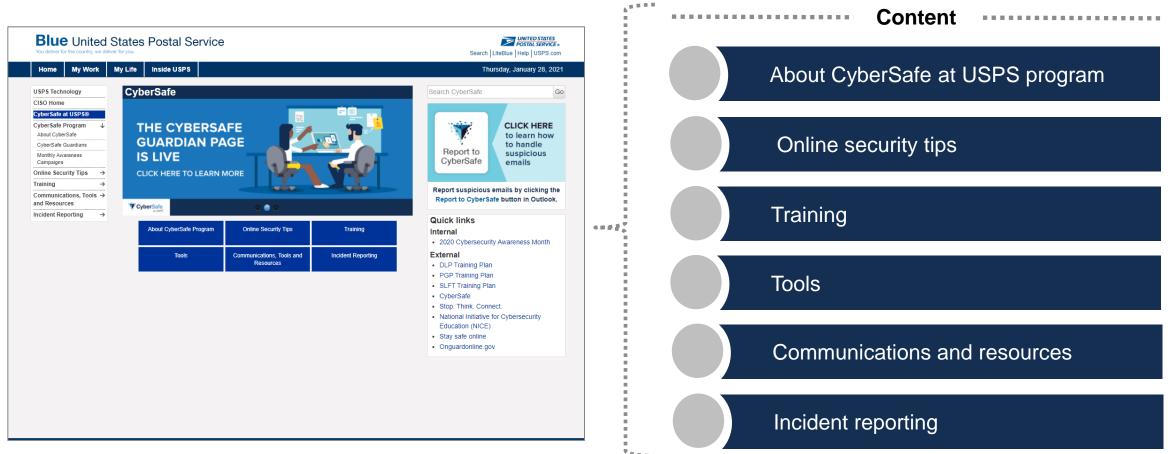


Resources

Empowering a culture of cybersecurity across the mailing ecosystem



CyberSafe at USPS®

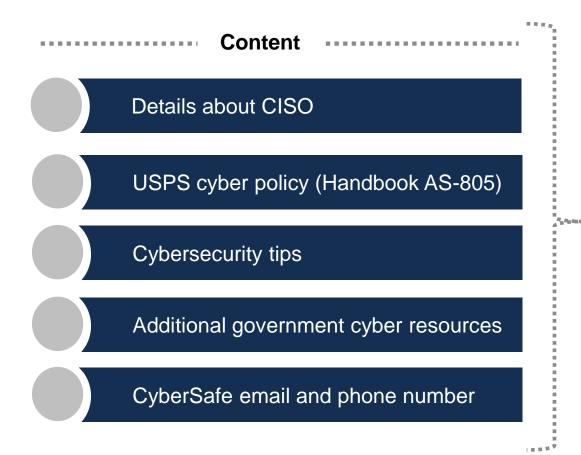


CyberSafe at USPS Website





USPS[®] PostalPro™





USPS PostalPro Website





Q&A



Thank You