Welcome to the CyberSecure My Business Webinar Series
We will begin promptly at 2pm EDT
All speakers will be muted until that time

Registration is now open for the September 11th webinar
“SMB Cyber Basics: Where to Start”

Join NCSA and our partners to prepare for next month’s National Cyber Security Awareness Month. Learn about small business cybersecurity basics. Where do you start? What are some “quick wins” to send you down the path of increased security? What are small business-specific resources you can access for free? Resources are available to help you improve the cybersecurity of your business.

visit www.staysafeonline.org/events/

To watch previous webinars, check out our “Resources Library” at www.staysafeonline.org/resources/
NATIONAL CYBER SECURITY ALLIANCE
Email Authentication Basics

Moderated by
Daniel Eliot, Director
Small Business Programs
National Cyber Security Alliance

Corey Allert, Manager
Network Security
FedEx

Phoebe Rouge, Technologist
Bureau of Consumer Protection
Office of Technology Research and Investigation
Federal Trade Commission

Rizwan Qureshi, Director
Product Management
Trend Micro
Be a Part of Something Big

Get involved and promote a safer, more secure internet.

www.staysafeonline.org
Goal of 5-Step Approach
Is Resilience

Know the threats and \textbf{Identify} and \textbf{Protect} your assets

\textbf{Detect} problems and \textbf{respond} quickly and appropriately

Know what \textbf{recovery} looks like and prepare

Thanks to our National Sponsors

\textbf{MediaPRO} Cybersecurity & Privacy Education

\textbf{TREND MICRO} Initiative for Education

Corey Allert, Manager
Network Security
FedEx
How to identify SPAM and protect yourself

Corey Allert
Definitions

• **Spam** is the practice of sending unsolicited e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

• **Phishing** is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

• **Spoofing** is e-mail activity in which the sender address is altered to appear as though the e-mail originated from a different source. Email doesn't provide any authentication, it is very easy to impersonate and forge emails.

• **Ransomware** is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
Where does spam come from?

• Spam today is sent via “bot-nets”, networks of virus- or worm-infected personal computers in homes and offices around the globe.

• Some worms install a backdoor which allows the spammer access to the computer and use it for malicious purposes.

• Others steal credentials for public or small company email accounts and send spam from there.

• A common misconception is that spam is blocked based on the sending email address.

• Spam is primarily identified by sending IP address and content.
  • Attachment type
  • URL
Why is SPAM still effective?

• Because it works!

• Because patching is boring!

30% of phishing messages were opened.
13% of targets went on to click the attachment or link.

The same old vulnerabilities exist.

Most attacks exploit known vulnerabilities where a patch has been available for months, if not years.
85% of successful exploit traffic is from the top 10 vulnerabilities.
Ways to identify Spam/Phishing

• You don’t recognize the sender.
• You recognize the name, but the email address doesn’t match (e.g., From John Smith; email address phisher@spamnetwork.com).
• You are requested to validate ANY personal information, account information, etc.
• You are being notified of winning anything. Chances are you didn’t, and if you click the link, there’s no telling what you might “win.”
• You have received an invoice for something you did not buy
• You mouse over the link and it doesn’t match what you expect (e.g., an email from Computer Superstore, but the link shows www.ComputerNotSoSuperStore.com).
Email Sample #1

Dear Member,

We have recently updated our Online system to include multi socket layer secure authentication. This is intended to provide you with the best security possible when accessing your account. You will need to update your account information in order to continue using your card.

Please follow the link below to start the security update immediately:

https://update.downey savingsonline.com/onlineserv/Login.cgi

There is no need to reply to this email. Your ticket code is LT<11907753615X.

We apologize for any inconvenience this may cause and appreciate your patience and understanding.

Sincerely,
Downey Savings

http://www.downey savings.us.com/online/
Email Sample #1 (cont)

---

**Subject:** Required Security Update

**From:** DowneySavings

**To:** john.doe@comcomwell.com

---

This phish uses a very nice "logo" to help make the email look real.

---

**The email was not addressed to you, in this case "John Doe".**

---

**The link is not cut-and-paste.**

---

The use of technical terms such as this are used to scare you into acting. Hopefully your bank doesn't do this.

---

This URL does not match the link shown above. First "http" vs. "https" in the link above. Second, the domain name itself is different. If the displayed link and the URL are different be suspicious.

---

Sincerely,

Downey Savings

---

8/14/2018
Email Sample #2

Please Call Us Immediately About Suspicious Account Activity

This is not a promotional e-mail. Please call us immediately at 1-800-333-9145 regarding recent activity on your Discover Card Account. We’re available 24/7 to take your call.

Please disregard this e-mail if you’ve already called us since the date this e-mail was sent.

We appreciate your prompt attention to this matter.

Thank you.
Discover Card Fraud Prevention Security Department

© 2008 Discover Bank, Member FDIC
Email Sample #2 (cont)

This phish is sometimes known as "vishing" - a phone call (voice) based phishing email.

*Please Call Us Immediately About Suspicious Email*

The email was not addressed to you.

This is not a promotional email. Please call us immediately at 1-800-707-8945 regarding recent activity on your Discover Card Account. We’re available 24/7 to take your call.

Please disregard this email if you’ve already called us since the date this email was sent.

We appreciate you.

Thank you.

Discover Card Fraud Prevention Security Department

© 2016 Discover Bank, Member FDIC

There is no information that would indicate that the sender knows you, for example there is no "account ending with XXXXX" message, nor is there a date of the offending transaction.

Grammar error: "already call us" instead of "already called us".

Why would an email from Discover come from a Prodigy email account?
We’ve recently revised our Online Access Agreement and E-Sign Consent to make them easier to understand. We’ve also included more information about our services and added new terms.

You do not need to do anything to continue using our Online Banking services.

To see what’s changed, please visit https://www.wellsfargo.com/onlineupdates. This page provides an overview of the changes and includes a link to the Online Access Agreement and instructions for accessing the E-Sign Consent.

If you have questions after reading the agreement and consent, sign on at https://www.wellsfargo.com/questions to send a secure, encrypted email. (Please do not reply to this automated email.)

Sincerely,

Randy Thomas
Wells Fargo Online Customer Service
Email Sample #3 (cont)

We've recently revised our Online Access Agreement and made it easier to understand. We've also included new terms and services and added new features.

You do not need to do anything to continue using your Online Banking services.

To see what's changed, please visit [https://www.wellsfargo.com/onlineupdates](https://www.wellsfargo.com/onlineupdates). This page provides a list of the changes and includes a link to the Online Access Agreement instructions.

If you have questions after reading the agreement and consent, send a secure, encrypted message to [https://www.wellsfargo.com/questions](https://www.wellsfargo.com/questions) to send a secure, encrypted message. (Please do not reply to this automated email.)

Sincerely,

[Name]

The email itself is informational – you do not have to do anything. Phishers generally (not always) need you to respond quickly so they create some sense of urgency.

The links are click-on links, not cut-and-paste, these can be "faked".

Do you expect to receive an email such as this from your bank? If so, is this similar to previous ones? In this case it would be easy to type the URL into a browser if you are interested in checking out the information described.

The URL matches the displayed URL. It is an HTTPS link and goes to a good site "wellsfargo.com". But be careful the link displayed here can be "faked".
Good morning,

Please see the attached invoice and remit payment according to the terms listed at the bottom of the invoice. If you have any questions please let us know.

Thank you!

Darrick McDaniel
Accounting Specialist
The criminals want you to click [Options...] and turn macros on. Don't do it!
Email Sample #4 (contd)

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server. To receive your private key follow one of the links:
2. http://onion.to/

If all of these addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [blocks]
4. Follow the instructions on the site.

!!! Your personal identification ID: [blocks] !!!

"Locky" sets your wallpaper to make sure you know what to do next
NATIONAL CYBER SECURITY ALLIANCE
Email Authentication Basics

Phoebe Rouge, Technologist
Bureau of Consumer Protection
Office of Technology Research and Investigation
Email Authentication Basics

Phoebe Rouge
Federal Trade Commission
The problem with email

• Email was designed in the early history of the internet
  – Priority: make sure messages actually made it to the destination
  – Everything can be fake except destination address

• Phishing emails are a danger
  – To consumers who are tricked into divulging sensitive information
  – To the reputation of the businesses whose identities are spoofed
The problem with email (2)

- In general, impersonation scams are a widespread problem:

<table>
<thead>
<tr>
<th>Consumer Sentinel Top Fraud Complaints (2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>
The problem with email (3)

• What if there was a way to prevent these scam emails from ever showing up in consumer inboxes?
Email Authentication

• Since 2004, the FTC has been urging the adoption of domain-level authentication systems
  – Verify that an email actually comes from the domain identified in the “From” line of the message.
• Since then, several technologies have addressed the issue, among them:
  – SPF
  – DKIM
  – DMARC
Email Authentication (2)

• While you as an SMB might not set these up directly, it is important to know if your email provider supports them.

• These are not software, but internet standards, like HTTP (websites) or URLs (format of website addresses).
Email Authentication (3)

- They rely on the Domain Name System (DNS)
  - The “address book of the internet”
  - e.g. www.example.com to 192.168.100.54
  - But it can also store other types of info
SPF (Sender Policy Framework)

• A way to “whitelist” the servers allowed to send email for your domain

• Analogy: Validating that the return address on a package actually is the address you expect it to be sent from
  – If you get a package from company ABC in Nevada, but the return address is from Illinois, it becomes suspicious
DKIM (Domain Keys Identified Mail)

• Uses digital signatures to confirm a message has not been tampered with or forged

• Analogy: “Signed and Sealed Envelope”
  – If the seal is broken, you know there may have been tampering
  – If the signature looks different than usual, it becomes suspicious
DMARC

- SPF and DKIM can flag a message as suspicious
- Still up to the receiver to decide what to do with it
- DMARC gives you a way to:
  - Indicate what you want recipients to do with suspicious mail from your domain (nothing, spam folder, reject)
  - Get reports whenever a suspicious mail is sent supposedly from your domain
- Analogy: “if you get a suspicious package that looks like it is from us”
  - Don’t open it
  - Call us to report it
Most Takes Place “Behind the Scenes”
Email Survey Results

Use of Email Authentication by Domains Studied

- SPF 86%
- No SPF 14%

DMARC Policy for Domains with SPF

- 66% No DMARC
- 23% none
- 2% quarantine
- 9% reject
Hosting Survey Results

Set by default
Configured independently
Not supported

9% SPF
18% DKIM
73% DMARC
Takeaways

• Email is easy to fake, and phishing is a threat to consumers and to businesses’ reputation

• Email Authentication can offer protection
  – SPF
  – DKIM
  – DMARC

• Check with your email service provider/marketer whether they offer/use these features
NATIONAL CYBER SECURITY ALLIANCE
Email Authentication Basics

Rizwan Qureshi, Director
Product Management
Best Practices for Email Authentication

1. Implement both SPF and DKIM on top-level domains and subdomains used for sending emails
2. For SPF records, optimize to less than 10 DNS queries
3. To avoid blocking legitimate emails, implement DMARC initially in “monitor” mode \((p=none)\) to get recipient’s feedback and verify satisfactory implementation of SPF and DKIM, next use policy “\(p=quarantine\)”, and eventually use the strictest policy “\(p=reject\)”.
4. Use DMARC’s reporting capabilities: RUA for telemetry into mail servers and RUF for failed and spoofed reports
5. Use *opportunistic* or *forced* TLS to protect email in transit between mail servers
Report on Email Authentication Results

Domain-based Authentication Details

Domain-based Authentication Details for test3.com – Last 12 Months

290 SPF  224 DKIM  1,070 DMARC

SPF  DKIM  DMARC - SPF  DMARC - DKIM  DMARC - Alignment  DMARC - Availability
Big Picture: There is no silver bullet to Protection

**LEGEND**
- Known Good
- Known Bad
- Unknown

- **Sender Authentication** & Reputation
- Spam Content Analysis & Correlation
- Anti-Malware & URL Reputation

- **Machine Learning (Anti-Malware)**
- **Machine Learning & Expert Sys (Fraud/BEC)**

- **Document Exploit Detection / Macro Analysis**

- **Sandbox Analysis**
- Real-time URL Analysis at Click Time

- **Malicious emails blocked**

- **Safe emails allowed**
For more information …

• [https://dmarc.org/](https://dmarc.org/)
• Online Trust Alliance: [https://otalliance.org/dmarc](https://otalliance.org/dmarc)
• M3AAWG: [https://www.m3aawg.org/categories/dmarc](https://www.m3aawg.org/categories/dmarc)
NATIONAL CYBER SECURITY ALLIANCE

Email Authentication Basics

Moderated by Daniel Eliot, Director Small Business Programs National Cyber Security Alliance

Corey Allert, Manager Network Security FedEx

Phoebe Rouge, Technologist Office of Technology Research and Investigation Federal Trade Commission

Rizwan Qureshi, Director Product Management Trend Micro
PUMPKIN SPICE LATTES, HALLOWEEN AND NATIONAL CYBERSECURITY AWARENESS MONTH

National Cybersecurity Awareness Month

LEARN MORE staysafeonline.org/ncsam
Use #CyberAware in all your tweets!
Like us on Facebook (/StaySafeOnline) to view live segments with experts each week and follow us on Twitter (@StaySafeOnline) for the latest news, resources and more.

Register yourself and/or your organization as a Champion to take action in support of NCSAM. It’s easy and FREE to sign up at https://staysafeonline.org/ncsam

Join our weekly Twitter discussion each Thursday in October at 3 p.m. EDT/Noon PDT.
Webinar Series
Second Tuesdays
2:00 p.m. EDT

Up-Coming Webinar Topics:
• September 11 “Cyber Basics”
• October 9 “Small Business Scams”
• November 6 “Cybersecurity Insurance”

To Register: www.staysafeonline.org
Email Authentication Basics

Federal Trade Commission
www.FTC.gov/smallbusiness

Trend Micro
www.trendmicro.com

FedEx Small Business Center
https://smallbusiness.fedex.com/home.html

National Cyber Security Alliance
www.staysafeonline.org/cybersecure-business