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 June 12th webinar
“Learn How to Assess Vendor Security”
visit www.staysafeonline.org/events/

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

Learn How to Protect Your Business Email Accounts Against Cyber Threats

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

Allison Lefrak, Attorney
Division of Privacy and Identity Protection
Federal Trade Commission

Jeroen Kemperman, Product Manager
Google
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 **Identify** and **Protect** your assets

**Detect** problems and **respond** quickly and appropriately

Know what **recovery** looks like and prepare

**Thanks to our National Sponsors**

[MediaPRO](#) Cybersecurity & Privacy Education

[TREND MICRO](#) Initiative for Education "DIGITAL SAFETY OUTREACH"
NATIONAL CYBER SECURITY ALLIANCE

Learn How to Protect Your Business Email Accounts Against Cyber Threats

Allison Lefrak, Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
Protecting Business Email

Allison Lefrak
Senior Staff Attorney
Federal Trade Commission
alefrak@ftc.gov
Phishing is when fraudsters mimic a legitimate business to trick people into giving out their personal information or money.
HOW CAN BUSINESSES BE VICTIMS OF PHISHING SCAMS?
WHAT SHOULD YOU DO IF YOUR BUSINESS HAS BEEN IMPERSONATED?

CONTACT AFFECTED CUSTOMERS

- Social media?
- If email, NO HYPERLINKS!
- Warn customers to be on the lookout for phony email.
- Remind them that legitimate businesses like yours won’t ask for personal information by email or text
WHAT SHOULD YOU DO IF YOUR BUSINESS HAS BEEN IMPERSONATED?

CONTACT LAW ENFORCEMENT

If consumers gave personal information or money, send them to IdentityTheft.gov for a personal recovery plan.
WHAT SHOULD YOU DO IF YOUR BUSINESS HAS BEEN IMPERSONATED?

HELP VICTIMS

- Report it to the Internet Crimes Complaint Center, ic3.gov
- File a complaint with the FTC, ftc.gov/complaint
- Forward phishing emails to Anti Phishing Working Group, reportphishing@apwg.org
WHAT IS MALWARE?

• Any piece of software that was written with the intent of doing harm to data, devices or to people.

• Common types include –
  • Virus
  • Trojans
  • Spyware
  • Worms
  • Ransomware
  • Adware
  • Botnets
AVOIDING MALWARE

• Educate your employees:
  • Do not open attachments in email unless you know who sent it and what it is.
  • Instead of clicking a link in an email, type the URL of a trusted site directly into your browser.
  • Talk about safe computing.
  • Run test drills.
• Report phishing attempts and malware to the FTC.
• Visit business.ftc.gov for information about protecting your business.
• Read Start with Security and Stick with Security for to-the-point tips on safeguarding sensitive data.
• Show FTC information security videos at your next staff meeting.
• Subscribe to the FTC Business Blog at ftc.gov/subscribe.
• Sign up for FTC scam alerts at ftc.gov/subscribe.
• Let us know what we can do to help you protect your business.
NATIONAL CYBER SECURITY ALLIANCE

Learn How to Protect Your Business Email Accounts Against Cyber Threats

Jeroen Kemperman, Product Manager
Google
The Anatomy of Account-Takeover

Presenter: Jeroen Kemperman
Author: Grzegorz Milka
Online accounts are valuable targets

Financial data
Personal data
Contacts
Identity (impersonation)
Data breaches are always there

Dropbox data breach: 68 million user account details leaked

Yahoo Says 1 Billion User Accounts Were Hacked

LinkedIn Lost 167 Million Account Credentials in Data Breach
And so are targeted hijacks

https://techcrunch.com/2017/08/23/i-was-hacked/
Modern password authentication requires a risk-aware, defense-in-depth system.
Password theft ecosystem
The three avenues of password theft

- Data breach
- Malware (Keyloggers)
- Phishing
Commoditization of abuse
The wares on sale

Data breach market

Keyloggers

Phishing kits

Research at Google
Markets can be tracked

In 2016, we have collected over 4000 data breach dumps with over 3.3B credentials.
Users reuse passwords

12%-43%*

reuse rate

**“Data breaches, phishing, or malware?”**
Users reuse passwords

17%* reuse rate

* internal estimate
Number of valid Google passwords found in data breaches:

67 Million
Volume of credentials stolen in 2016*

- Data breaches: >3.3B
- Keyloggers: >1M
- Phishing: >12M

*all services, lower bound
Hijacking likelihood*

Compared to a general active account, how much more likely it is that you will be a victim of hijacking if we know:

- You were in a breach: >10x
- Had a keylogger: >40x
- Were phished: >500x

*lower bound
Prevention
Sign-in risk detection
Challenges
Modern password authentication requires a risk-aware, defense-in-depth system.
has shared a document on Google Docs with you

has invited you to view the following document:

Open in Docs

Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information.

Click here to Reply, Reply to all, or Forward
Safe Browsing

Deceptive site ahead

Attackers on esty.adelawarriewood.com.au may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

✓ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

DETAILS  Back to safety
We notify compromised users and ask them to change their password.
Prevention
Sign-in risk detection
Challenges
Password-only authentication is risky.
Adoption of additional security is low

<10% 2FA

~12% Password managers*

Of active Google accounts

Of Americans
*Pew Research Center
Bridging the gap between 2FA and passwords

Image courtesy of Dr Frank Stajano, “Passwords and the Evolution of Imperfect Authentication”
Dimensionality of risk

How surprised we are to see you login like that?

Unusual location, device, time

How suspicious does the login look?

- Similarity to known hijacking patterns
- Is user at risk?
But... Hijackers adapt.
In the end, we don’t look at user’s location for many users.
Prevention
Sign-in risk detection
Challenges
“Dynamic 2FA”
Asking for additional verification

When the sign-in is risky

That is solvable by the user

Research at Google
Modern password authentication requires a risk-aware, defense-in-depth system.
2 things that can go wrong

Hijacker gets in

User is locked out
Choose the challenge that minimizes damage

- Allow
- MAIL VERIFICATION
- SMS CODE
- GOOGLE PROMPT
- Deny
Secondary e-mail verification

10% Of users have problems passing this challenge
Secondary e-mail verification

Vulnerable to password reuse
SMS code

Vulnerable to phishing...
18% of observed phishing kits collect phone data.

... and other methods
There are multiple ways to get the SMS code besides phishing.
Google Prompt

Nothing stops the user from just clicking “Yes”

More flexible

We can present more data and use additional signals for risk-analysis
In-session detection
Hijackers need to monetize

- Theft of personal data
- Viral-phishing and scams
- Spamming and product abuse
First we bring the user into the loop
Finding the hijacker in-session

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>20:54:24</td>
<td>LOGIN (new)</td>
<td></td>
</tr>
<tr>
<td>20:55:51</td>
<td>MAIL_DELETE</td>
<td>1 (new device notifn.)</td>
</tr>
</tbody>
</table>
## Finding the hijacker in-session

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>20:54:24</td>
<td>LOGIN (new)</td>
<td></td>
</tr>
<tr>
<td>20:55:51</td>
<td>MAIL_DELETE</td>
<td>1 (new device notification)</td>
</tr>
<tr>
<td>21:01:30</td>
<td>EXPORT_CONTACTS</td>
<td></td>
</tr>
</tbody>
</table>
Finding the hijacker in-session

20:54:24 | LOGIN (new) |
20:55:51 | MAIL_DELETE | 1 (new device notifn.)
21:01:30 | EXPORT_CONTACTS |
21:06:45 | MAIL_SEND | with phishing links
21:07:50 | MAIL_FILTER | “hacked”->Trash
21:08:07 | LOGOUT |
Modern password authentication requires a **risk-aware,** **defense-in-depth** system.
Take steps now to protect your business email

- Develop a cybersecurity plan for your small business
  - Resource: https://www.fcc.gov/cyberplanner
- Verify to Clarify
- Encrypt email
- Use strong authentication
- Don’t forget mobile devices
- Train employees on safe email usage
- Don’t forget physical security
- Know who to turn to

“Never leave that till tomorrow which you can do today.” –Ben Franklin
NATIONAL CYBER SECURITY ALLIANCE

Learn How to Protect Your Business Email Accounts Against Cyber Threats

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

Allison Lefrak, Attorney
Division of Privacy and Identity Protection
Federal Trade Commission

Jeroen Kemperman, Product Manager
Google
Webinar Series
Second Tuesdays
2:00 p.m. EDT

Up-Coming Webinar Topics:

• June 12th How to Assess Vendor Security
• July 10th Cybersecurity Insurance

To Register: www.staysafeonline.org
NATIONAL CYBER SECURITY ALLIANCE

Learn How to Protect Your Business Email Accounts Against Cyber Threats

Federal Trade Commission
www.FTC.gov/smallbusiness

Google
https://privacy.google.com/take-control.html

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