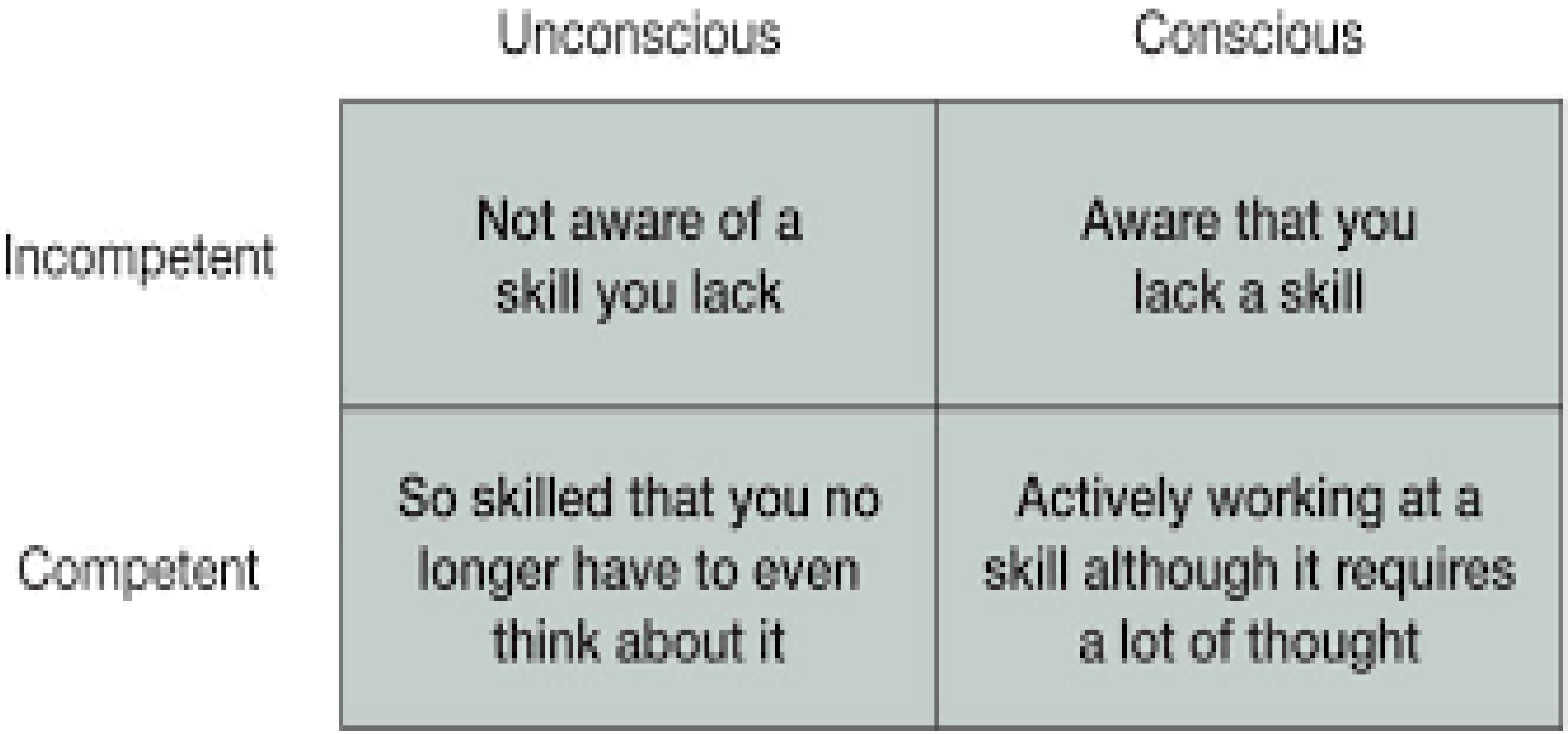
Internet Security

November 12, 2016

“Just because you are paranoid doesn’t mean they aren’t out to get you”

Four Stages of Competence



	Unconscious	Conscious
Incompetent	Not aware of a skill you lack	Aware that you lack a skill
Competent	So skilled that you no longer have to even think about it	Actively working at a skill although it requires a lot of thought

Internet Security

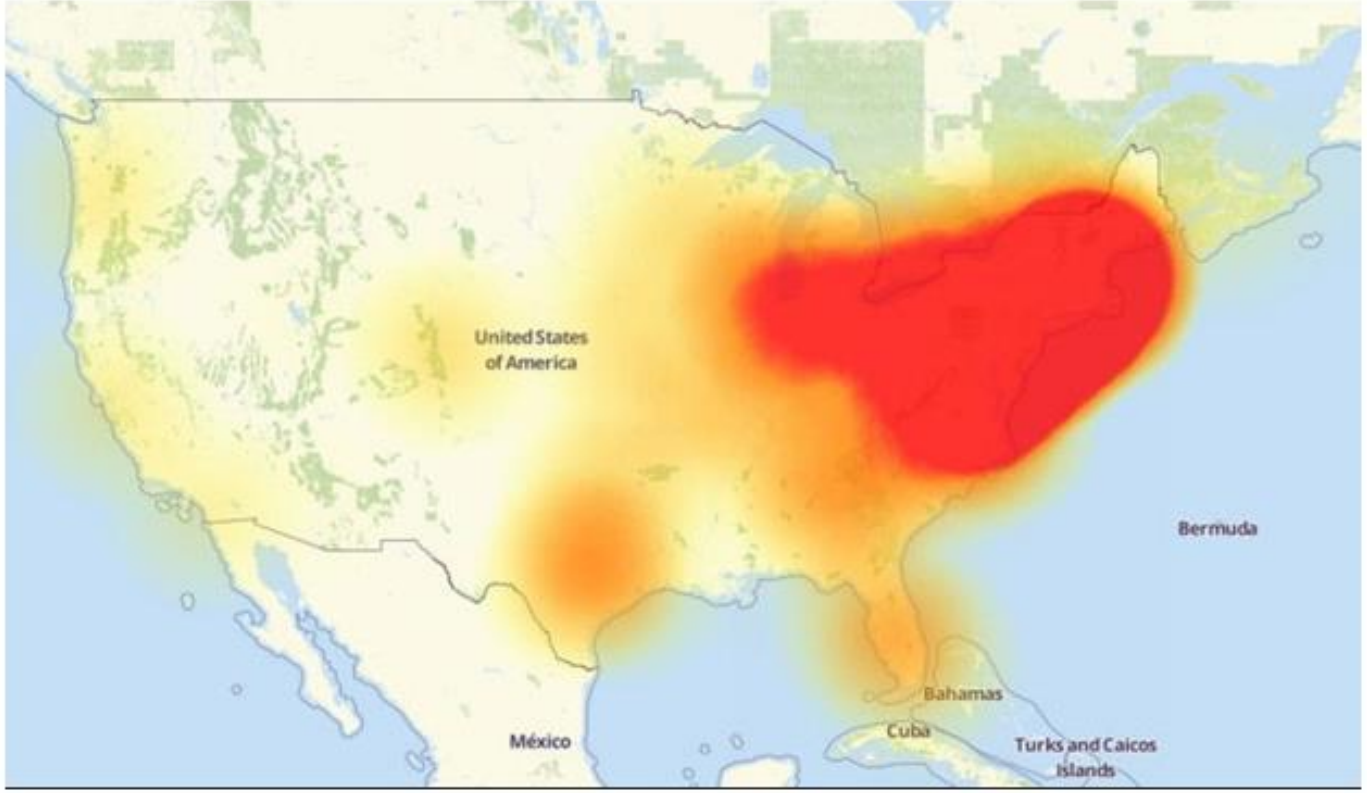
Step One: Learn / understand the risks we face

Step Two: Learn / implement countermeasures

Internet Security Threats @ 30,000 Feet

- Weisman - “Where are the real cybersecurity threats?”
- McGill – “The Inevitability of Being Hacked”
- October hack disrupts Internet service in eastern U.S.

Hack disrupts Internet service in large parts of East Coast, Midwest (October 21, 2016)



Internet Security Threats @ 30 Feet

- Our devices may become part of a “bot-net”
- Personal information may be encrypted / stolen / abused
- Device performance may be compromised
- Our identity may be stolen
- We may be scammed, to our detriment
- (Note that these threats may also involve other channels)
- Distributed Denial of Service (DDoS) attack (unlikely)

Internet Security Threats @ 30 Feet

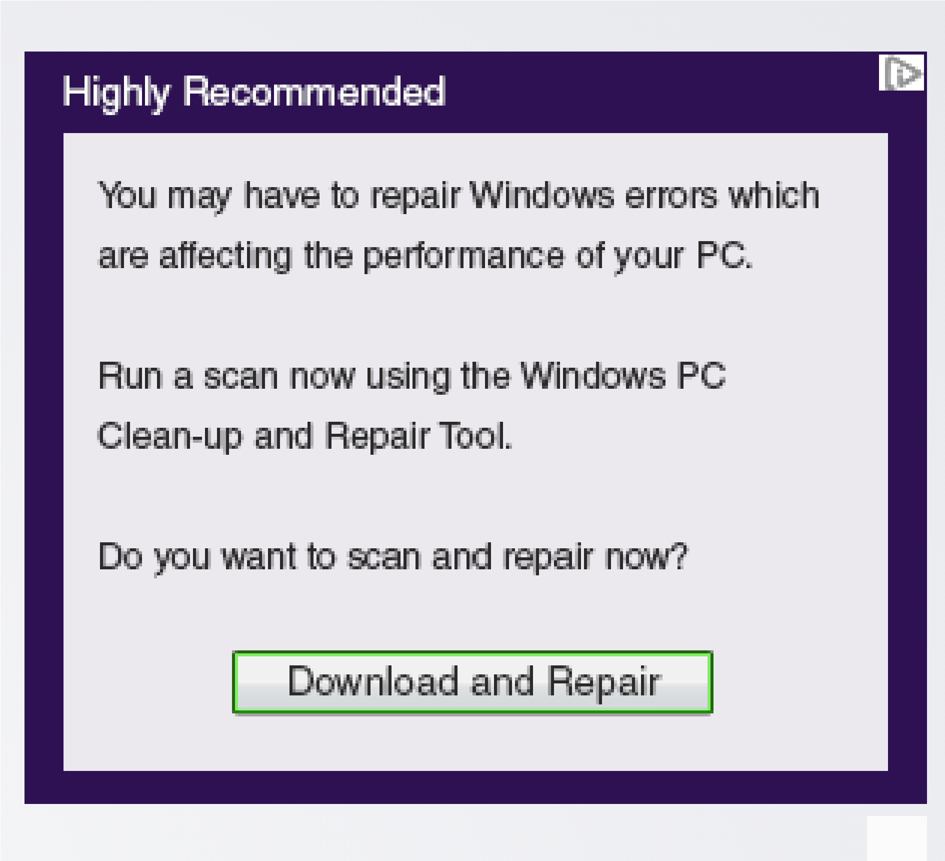
- Man-in-the-Middle (MITM) exploits
- Software exploits – install malware on your device(s)
  - Bot-net
  - Keystroke logger / webcam / microphone
  - Other
- Phishing (can lead to all sorts of bad things)
- (See Phishing examples)
- Other?

Example #1 – Phony Microsoft Pop-Up

- An LCACE member was recently “phished”
- She had a “Microsoft” pop-up reporting malware
- Was told to call a 1-800 number for assistance
- Did so, and was offered “assistance” for a fee
- Her contact asked for the pop-up code number
- Our member declined and hung up
- In a previous incident another LCACE member paid

Example #2 – Phony Windows Pop-Up

A phishing “pop-up” in my Google Chrome browser as I was reading email; November 9, 2016)



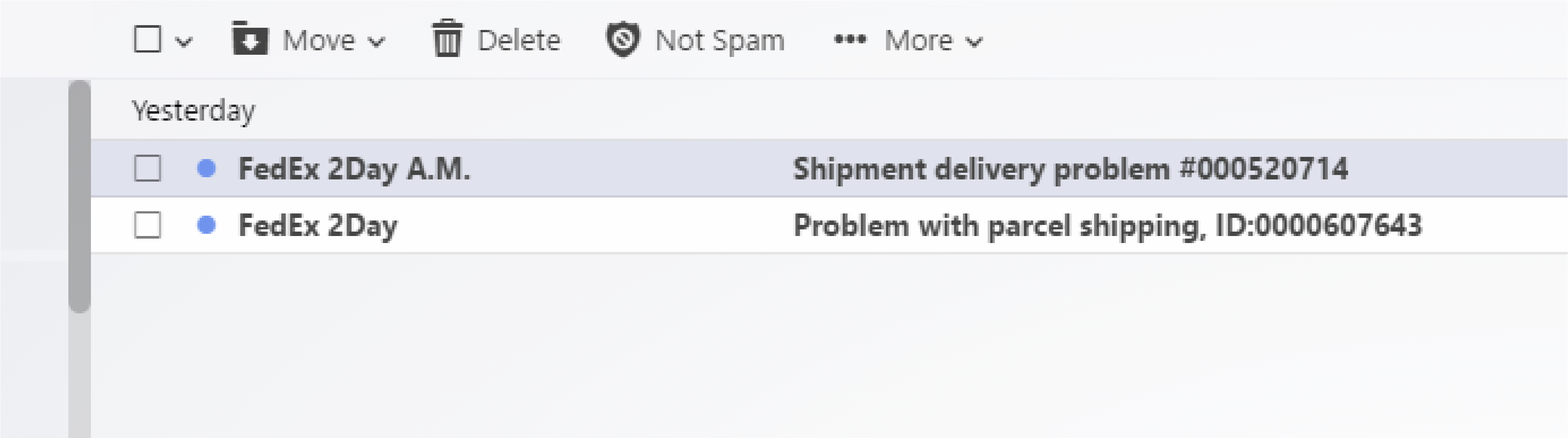
Highly Recommended

You may have to repair Windows errors which are affecting the performance of your PC.

Run a scan now using the Windows PC Clean-up and Repair Tool.

Do you want to scan and repair now?

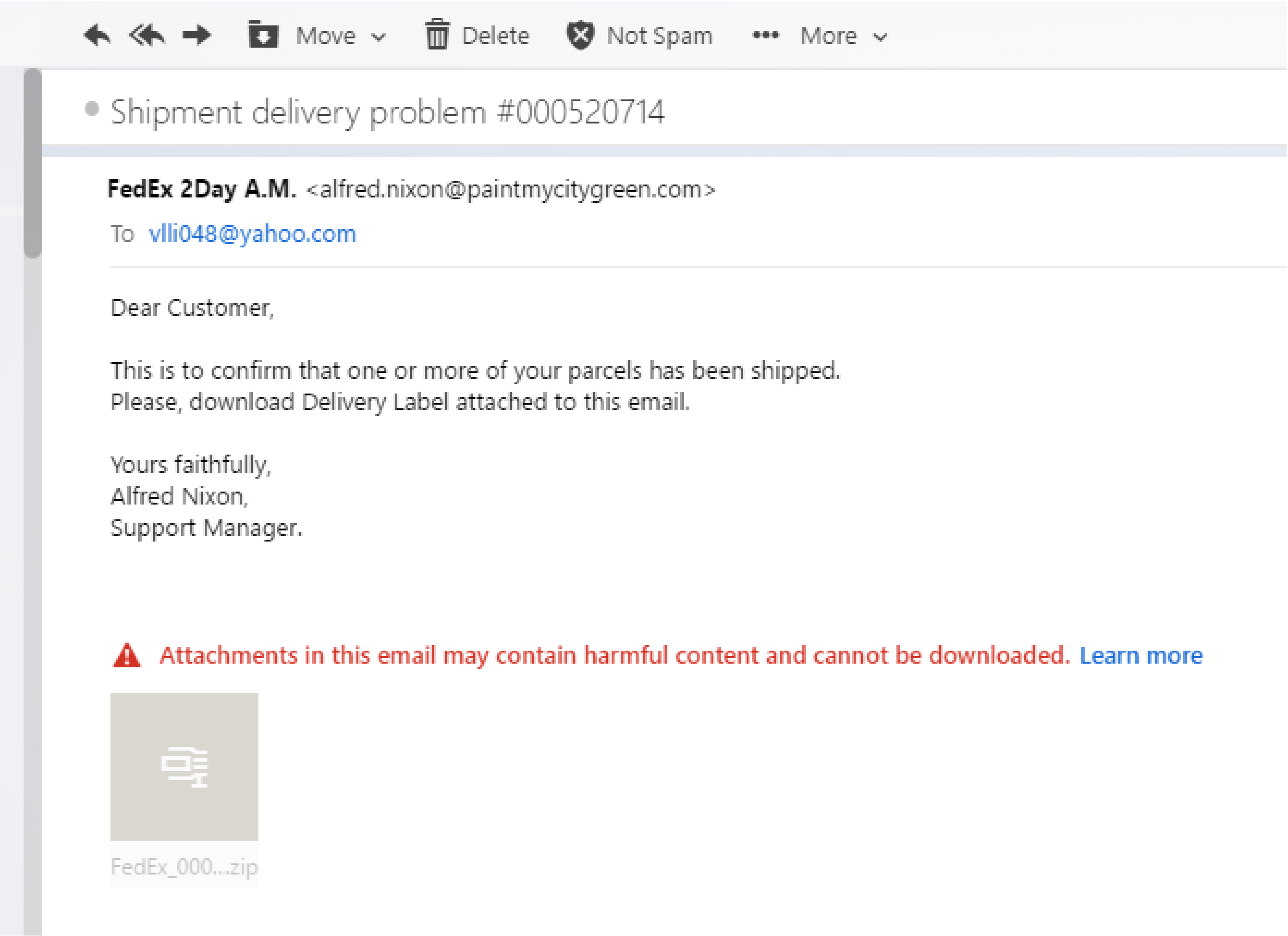
Example #3 – Spam Email



Yesterday

□ ● FedEx 2Day A.M. Shipment delivery problem #000520714

□ ● FedEx 2Day Problem with parcel shipping, ID:0000607643



Shipment delivery problem #000520714

FedEx 2Day A.M. <alfred.nixon@paintmycitygreen.com>

To vlli048@yahoo.com

Dear Customer,

This is to confirm that one or more of your parcels has been shipped.
Please, download Delivery Label attached to this email.

Yours faithfully,
Alfred Nixon,
Support Manager.

Attachments in this email may contain harmful content and cannot be downloaded. Learn more

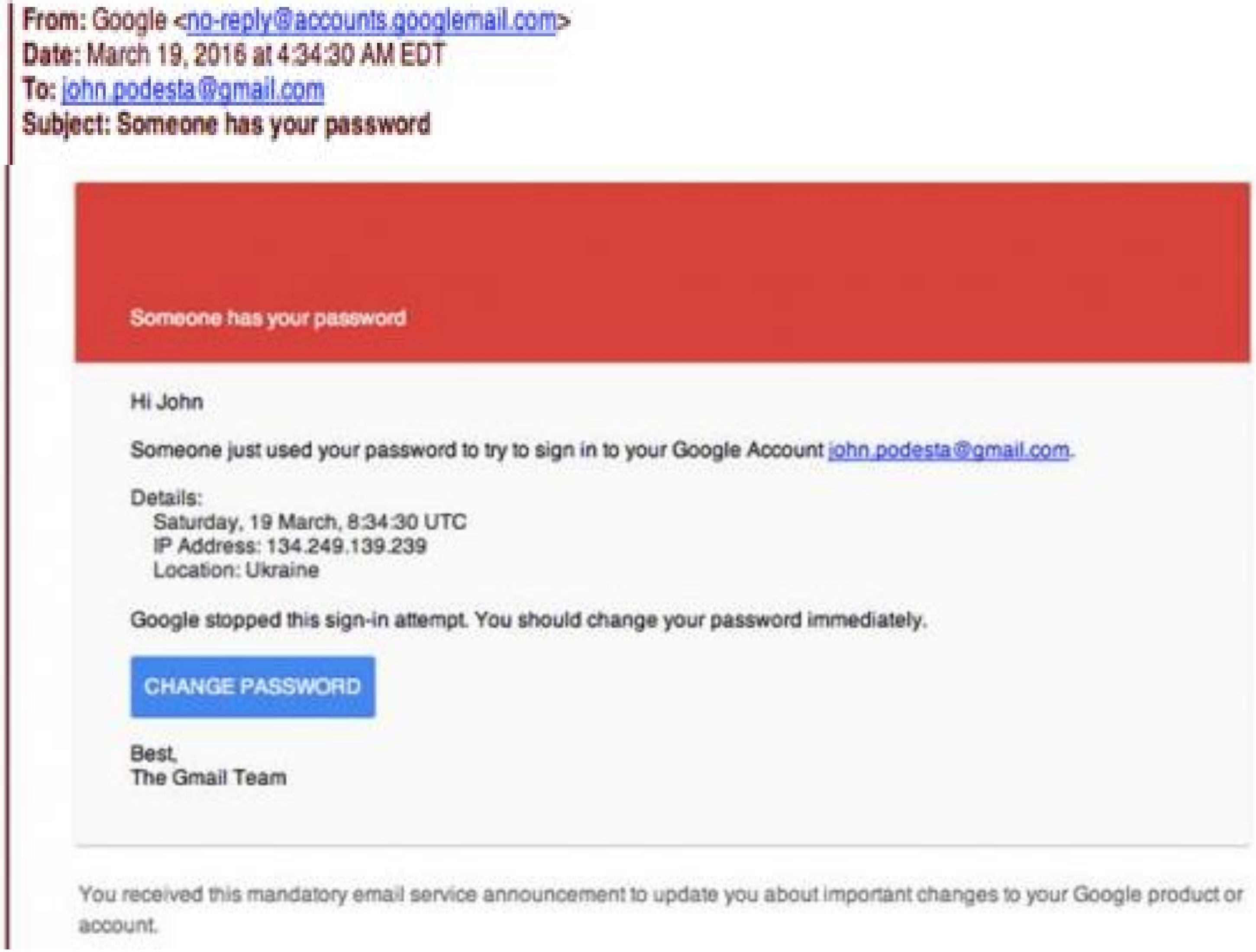
FedEx_000...zip

Example #4 - John Podesta Email Hack

- 50,000 HCA emails were stolen from his computer
- Contain sensitive information, potentially damaging
- Emails released in stages by Wiki-Leaks prior to election
- How were they stolen?
  - Disgruntled staffer?
  - HCA server hacked?
  - ISP / email provider hacked?
  - Phishing?

Example #4 - John Podesta Email Hack

- Podesta received email request to reset his Gmail password
- From: “no-reply@accounts.googlemail.com”
- Blue “CHANGE PASSWORD” button provided in email
- Forwarded to HCA internal computer-security dept.
- Staffer OK’d email & password change
- Also sent correct Google address for password change
- *Podesta or staffer clicked email link to update password*



From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Someone has your password

Hi John

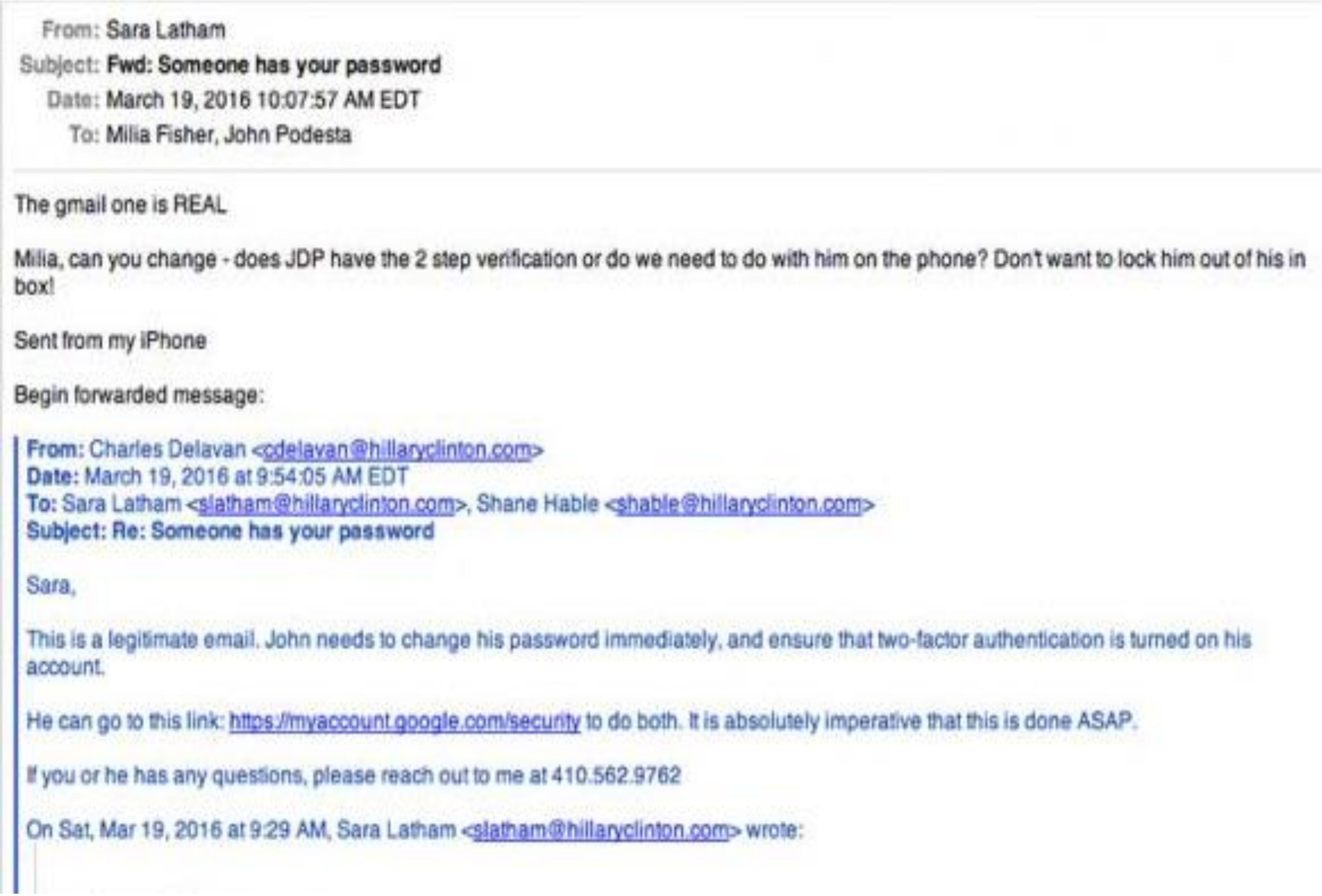
Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.



From: Sara Latham
Subject: **Fwd: Someone has your password**
Date: March 19, 2016 10:07:57 AM EDT
To: Milia Fisher, John Podesta

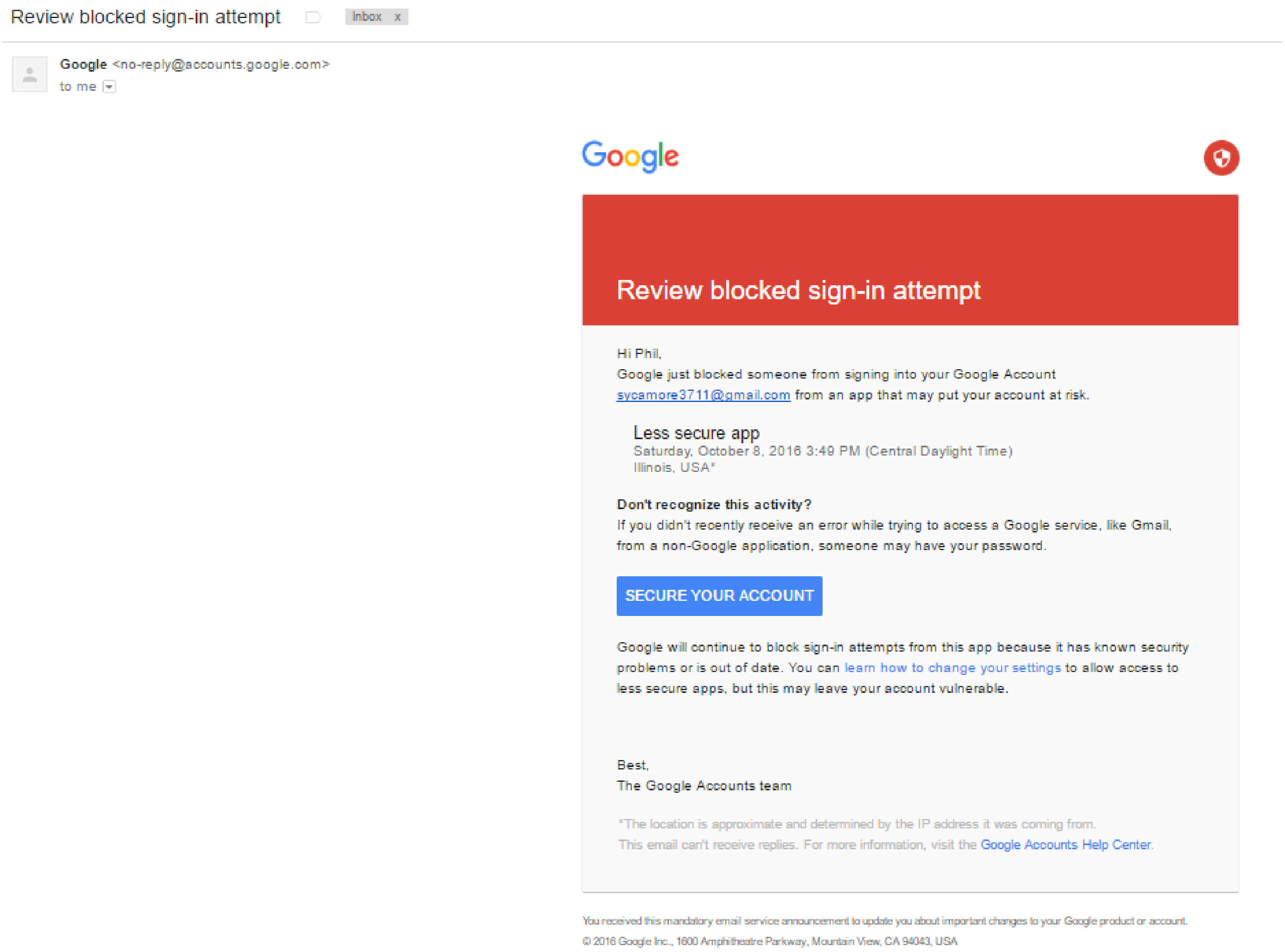
The gmail one is REAL

Milia, can you change - does JDP have the 2 step verification or do we need to do with him on the phone? Don't want to lock him out of his in box!

Sent from my iPhone

Begin forwarded message:

> **From:** Charles Delavan <cdelavan@hillaryclinton.com>
> **Date:** March 19, 2016 at 9:54:05 AM EDT
> **To:** Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
> **Subject: Re: Someone has your password**
>
> Sara,
>
> This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.
>
> He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.
>
> If you or he has any questions, please reach out to me at 410.562.9762
>
> On Sat, Mar 19, 2016 at 9:29 AM, Sara Latham <slatham@hillaryclinton.com> wrote:



Review blocked sign-in attempt

Google <no-reply@accounts.google.com>
to me

Review blocked sign-in attempt

Hi Phil,
Google just blocked someone from signing into your Google Account sycamore3711@gmail.com from an app that may put your account at risk.

Less secure app
Saturday, October 8, 2016 3:49 PM (Central Daylight Time)
Illinois, USA*

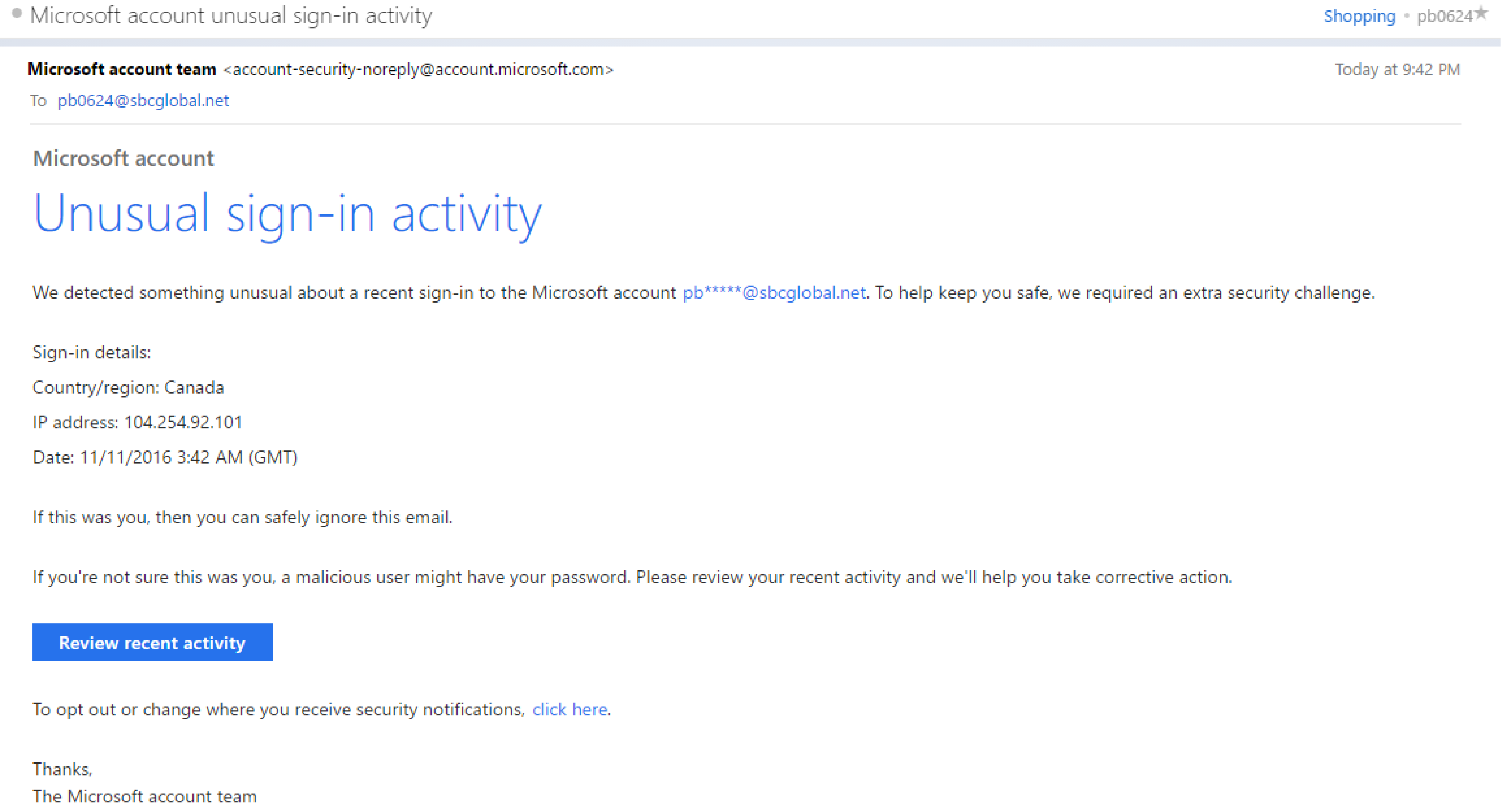
Don't recognize this activity?
If you didn't recently receive an error while trying to access a Google service, like Gmail, from a non-Google application, someone may have your password.

Google will continue to block sign-in attempts from this app because it has known security problems or is out of date. You can learn how to change your settings to allow access to less secure apps, but this may leave your account vulnerable.

Best,
The Google Accounts team

*The location is approximate and determined by the IP address it was coming from.
This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.



● Microsoft account unusual sign-in activity

Microsoft account team <account-security-noreply@account.microsoft.com>

Today at 9:42 PM

To pb0624@sbcglobal.net

Microsoft account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account pb*****@sbcglobal.net. To help keep you safe, we required an extra security challenge.

Sign-in details:

Country/region: Canada

IP address: 104.254.92.101

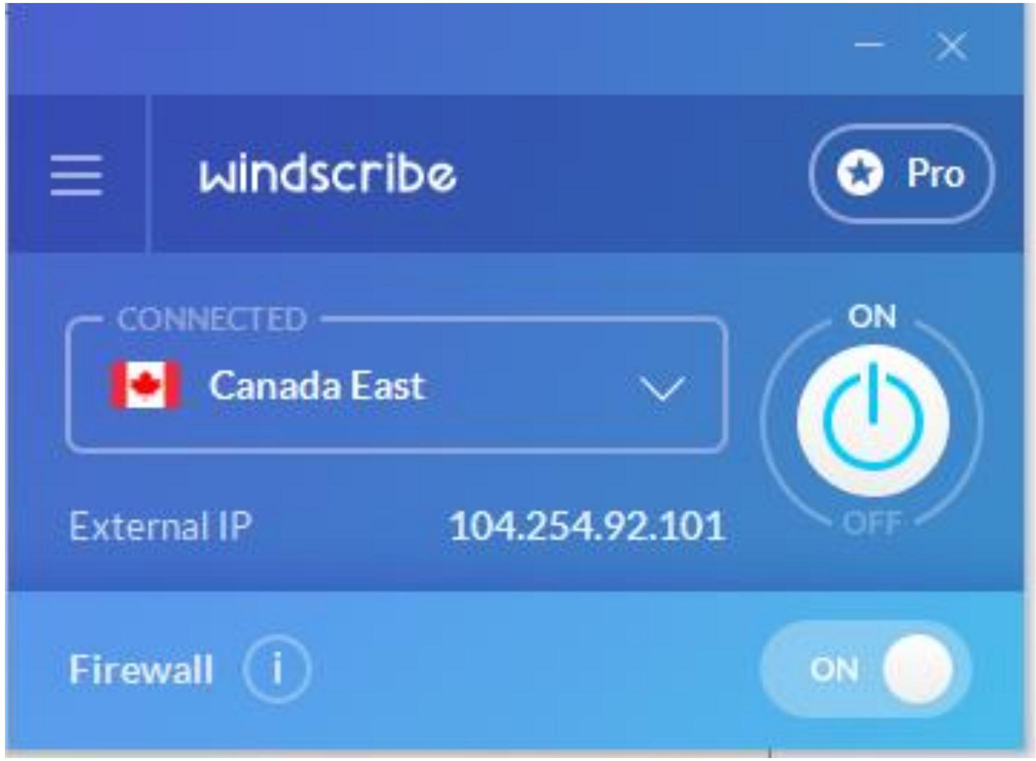
Date: 11/11/2016 3:42 AM (GMT)

If this was you, then you can safely ignore this email.

If you're not sure this was you, a malicious user might have your password. Please review your recent activity and we'll help you take corrective action.

To opt out or change where you receive security notifications, click here.

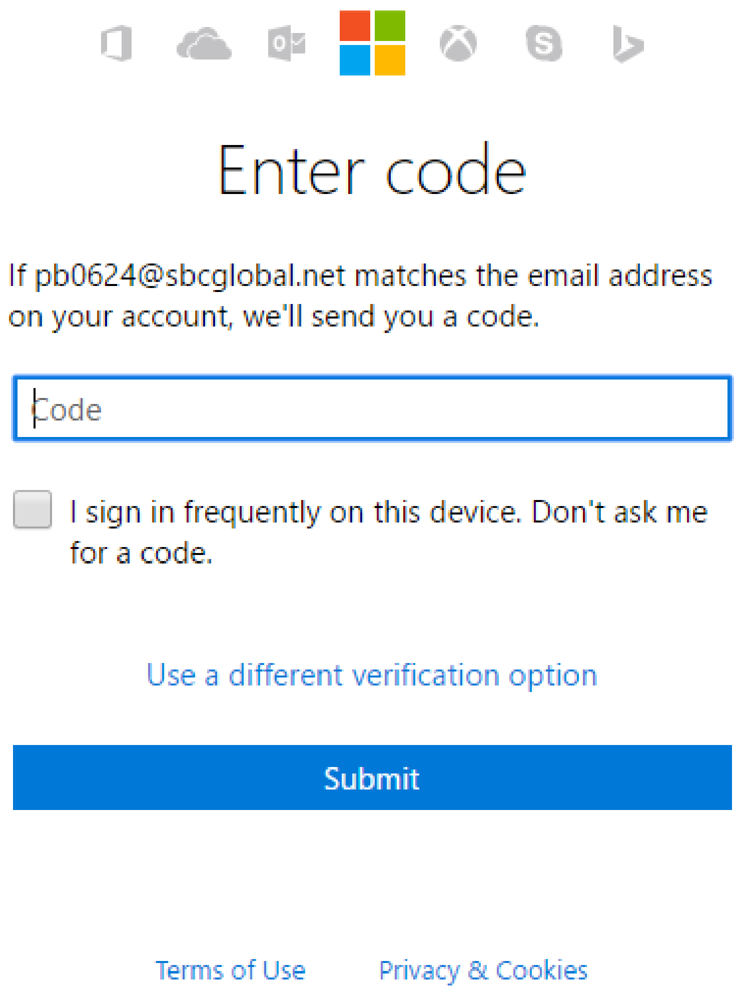
Thanks,
The Microsoft account team



CONNECTED
Canada East

External IP 104.254.92.101

Firewall ON

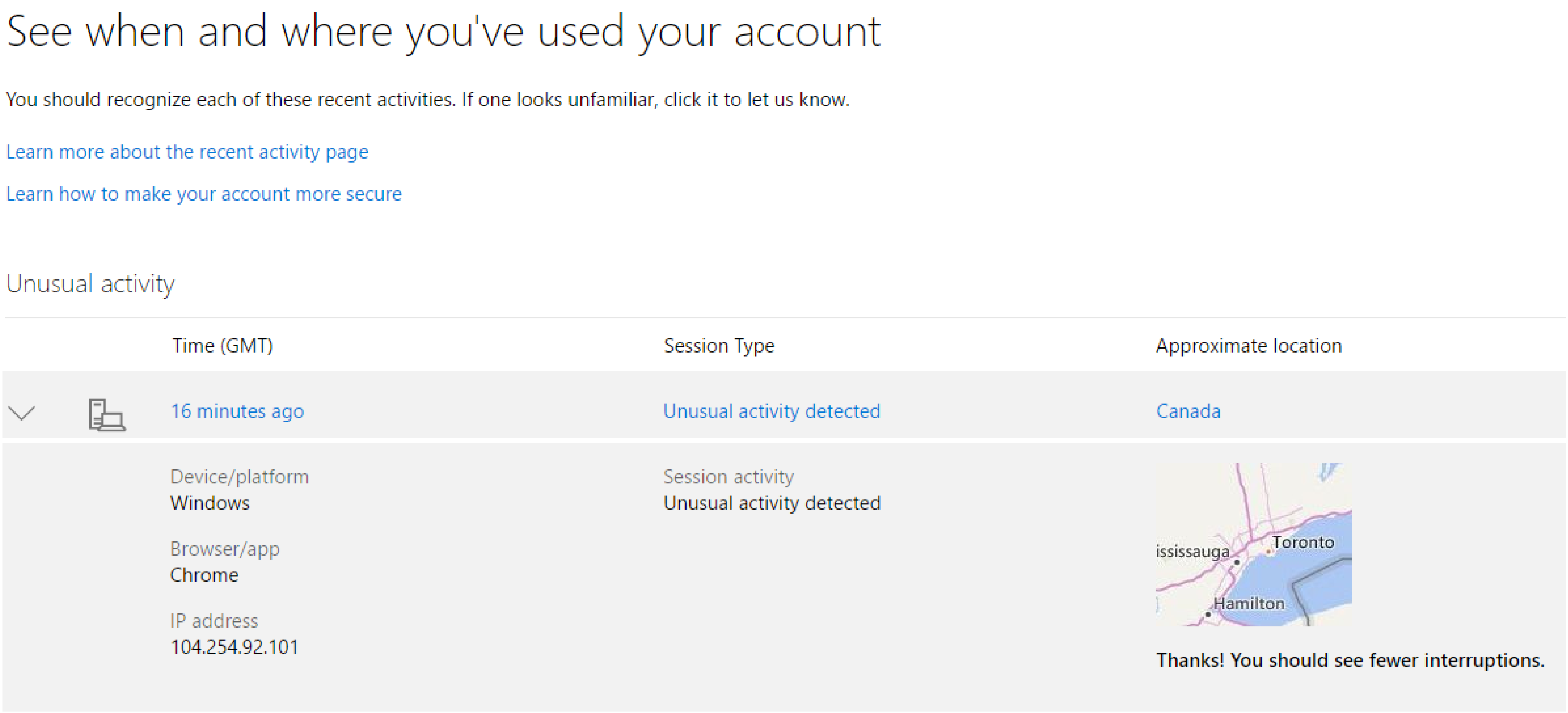


Enter code

If pb0624@sbcglobal.net matches the email address on your account, we'll send you a code.

Code

☐ I sign in frequently on this device. Don't ask me for a code.



See when and where you've used your account

You should recognize each of these recent activities. If one looks unfamiliar, click it to let us know.

Learn more about the recent activity page

Learn how to make your account more secure

Unusual activity

Time (GMT)	Session Type	Approximate location
16 minutes ago	Unusual activity detected	Canada

Device/platform
Windows

Browser/app
Chrome

IP address
104.254.92.101

Session activity
Unusual activity detected

Thanks! You should see fewer interruptions.

The risks of “Cloud” storage

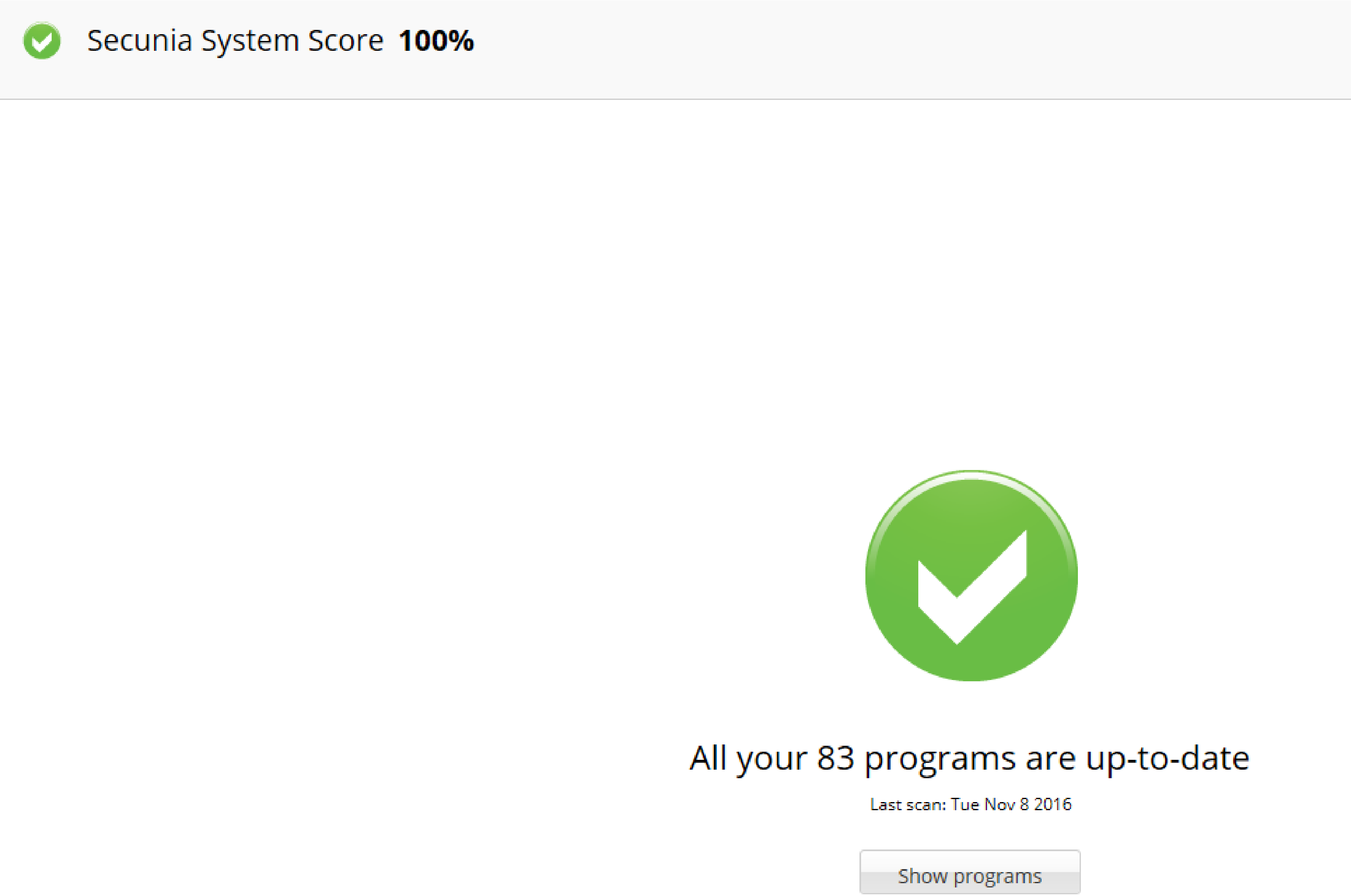
- Your information may be stolen during transmission
- Your information may be stolen from Cloud servers
- Those with whom you interact may sell your data
- Your files may be lost if the provider goes out of business
- Ownership of stored information may not be clear
- Back-up copies may not be deleted when you delete a file
- Government agencies may access your information

Current / Future Internet Security Environment

- “Bad Guys” driven by greed / ideology / national interest
- They are very capable & share “best practices”
- Bot-nets and exploits can be purchased or rented
- Bot-nets allow constant, widespread attacks
- The Internet allows operation from anywhere
- There is little on the horizon to slow them down
- Meanwhile, we are becoming more and more connected

What Should You Do?

- Use a network router; ensure your network is protected
- Use anti-virus / firewall software; keep updated
- Create complex, UNIQUE passwords – for everything!
- Ensure your OS and application software is up-to-date
- (Use Secunia PSI to monitor and auto-update)
- Use a Standard account for ALL web-surfing
- Use a Virtual Private Network (VPN)

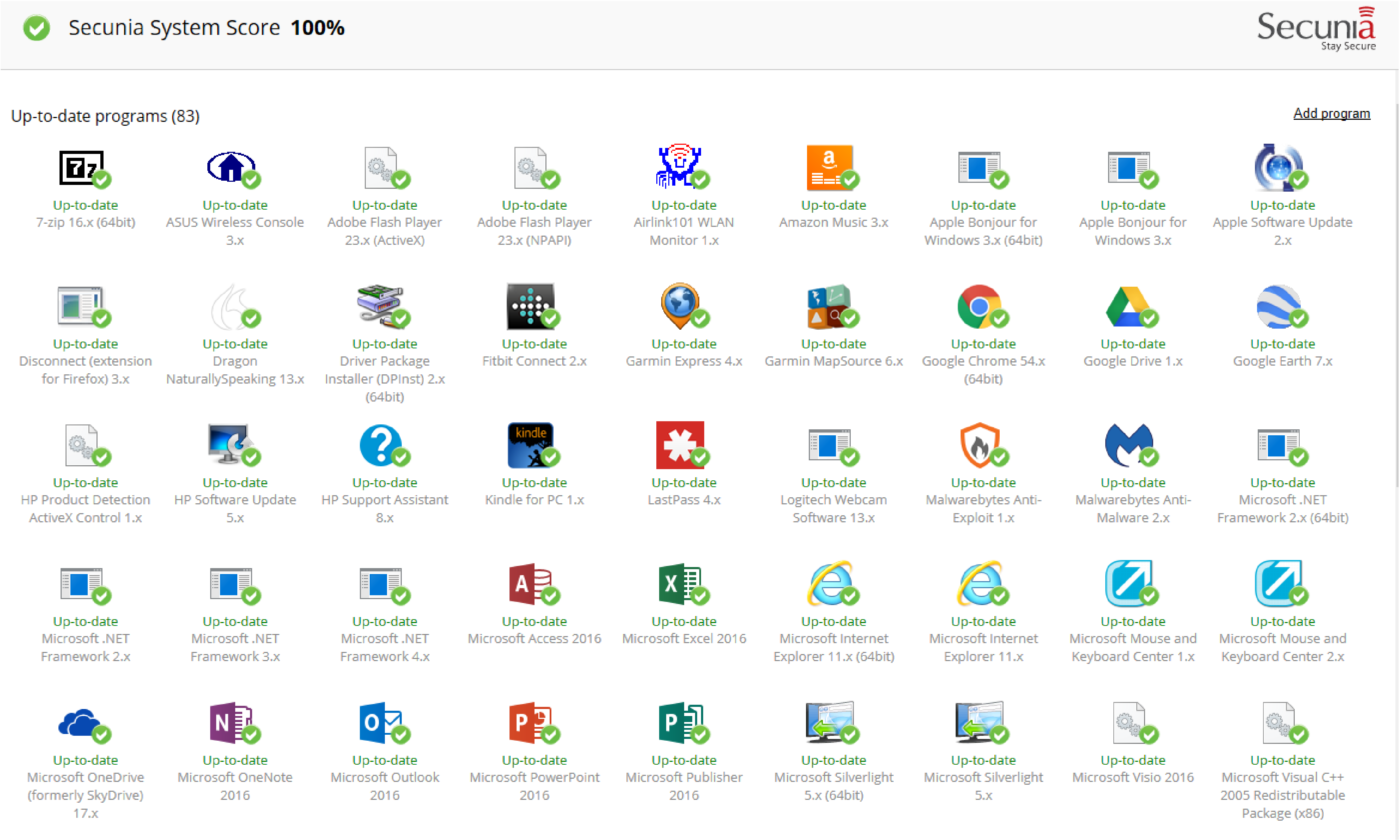


✓ Secunia System Score **100%**

✓

All your 83 programs are up-to-date

Last scan: Tue Nov 8 2016



Secunia System Score **100%**

Up-to-date programs (83)

Up-to-date
7-zip 16.x (64bit)

Up-to-date
ASUS Wireless Console 3.x

Up-to-date
Adobe Flash Player 23.x (ActiveX)

Up-to-date
Adobe Flash Player 23.x (NPAPI)

Up-to-date
Airlink101 WLAN Monitor 1.x

Up-to-date
Amazon Music 3.x

Up-to-date
Apple Bonjour for Windows 3.x (64bit)

Up-to-date
Apple Bonjour for Windows 3.x

Up-to-date
Apple Software Update 2.x

Up-to-date
Disconnect (extension for Firefox) 3.x

Up-to-date
Dragon NaturallySpeaking 13.x

Up-to-date
Driver Package Installer (DPInst) 2.x (64bit)

Up-to-date
Fitbit Connect 2.x

Up-to-date
Garmin Express 4.x

Up-to-date
Garmin MapSource 6.x

Up-to-date
Google Chrome 54.x (64bit)

Up-to-date
Google Drive 1.x

Up-to-date
Google Earth 7.x

Up-to-date
HP Product Detection ActiveX Control 1.x

Up-to-date
HP Software Update 5.x

Up-to-date
HP Support Assistant 8.x

Up-to-date
Kindle for PC 1.x

Up-to-date
LastPass 4.x

Up-to-date
Logitech Webcam Software 13.x

Up-to-date
Malwarebytes Anti-Exploit 1.x

Up-to-date
Malwarebytes Anti-Malware 2.x

Up-to-date
Microsoft .NET Framework 2.x (64bit)

Up-to-date
Microsoft .NET Framework 2.x

Up-to-date
Microsoft .NET Framework 3.x

Up-to-date
Microsoft .NET Framework 4.x

Up-to-date
Microsoft Access 2016

Up-to-date
Microsoft Excel 2016

Up-to-date
Microsoft Internet Explorer 11.x (64bit)

Up-to-date
Microsoft Internet Explorer 11.x

Up-to-date
Microsoft Mouse and Keyboard Center 1.x

Up-to-date
Microsoft Mouse and Keyboard Center 2.x

Up-to-date
Microsoft OneDrive (formerly SkyDrive) 17.x

Up-to-date
Microsoft OneNote 2016

Up-to-date
Microsoft Outlook 2016

Up-to-date
Microsoft PowerPoint 2016

Up-to-date
Microsoft Publisher 2016

Up-to-date
Microsoft Silverlight 5.x (64bit)

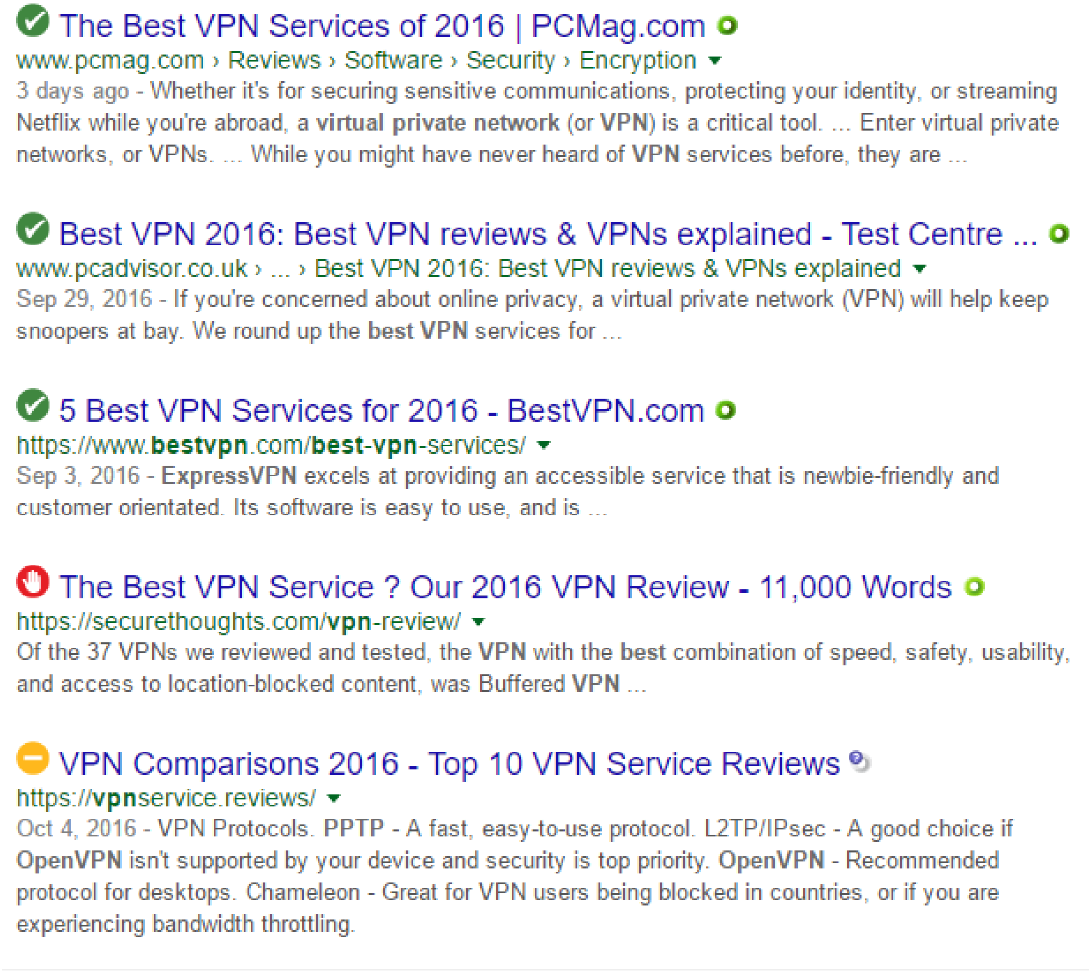
Up-to-date
Microsoft Silverlight 5.x

Up-to-date
Microsoft Visio 2016

Up-to-date
Microsoft Visual C++ 2005 Redistributable Package (x86)

What Should You Do?

- View Web filtering & Web of Trust before surfing the Web
- Use caution when transferring from site to site
- Be very careful before clicking on any links; think twice!
- As alternative to linking, go directly to desired site
- Use encryption for important (all?) files; ditto for email
- Implement Two-Factor Authentication (2FA)
- Routinely back up all your files
- Use only your own flash drives / keep them secure



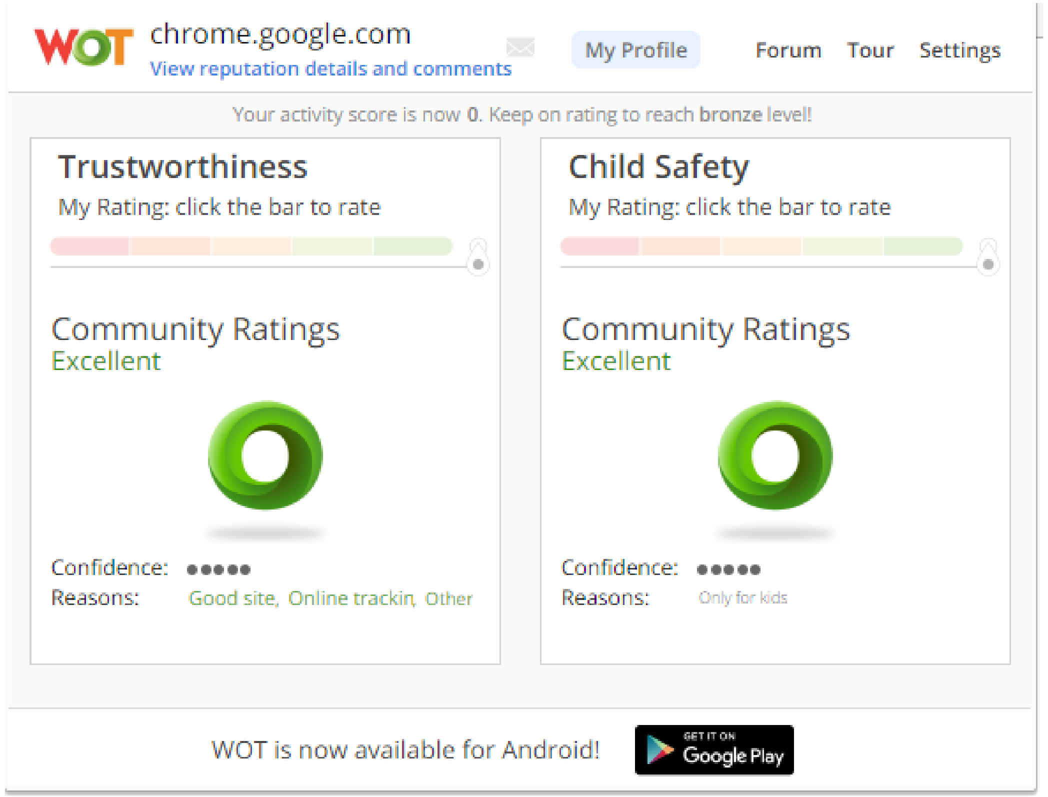
✓ The Best VPN Services of 2016 | PCMag.com ○
www.pcmag.com › Reviews › Software › Security › Encryption ▾
3 days ago - Whether it's for securing sensitive communications, protecting your identity, or streaming Netflix while you're abroad, a **virtual private network** (or **VPN**) is a critical tool. ... Enter virtual private networks, or VPNs. ... While you might have never heard of **VPN** services before, they are ...

✓ Best VPN 2016: Best VPN reviews & VPNs explained - Test Centre ... ○
www.pcadvisor.co.uk › ... › Best VPN 2016: Best VPN reviews & VPNs explained ▾
Sep 29, 2016 - If you're concerned about online privacy, a virtual private network (VPN) will help keep snoopers at bay. We round up the **best VPN** services for ...

✓ 5 Best VPN Services for 2016 - BestVPN.com ○
https://www.**bestvpn**.com/**best-vpn**-services/ ▾
Sep 3, 2016 - **ExpressVPN** excels at providing an accessible service that is newbie-friendly and customer orientated. Its software is easy to use, and is ...

✋ The Best VPN Service ? Our 2016 VPN Review - 11,000 Words ○
https://securethoughts.com/**vpn**-review/ ▾
Of the 37 VPNs we reviewed and tested, the **VPN** with the **best** combination of speed, safety, usability, and access to location-blocked content, was Buffered **VPN** ...

⊖ VPN Comparisons 2016 - Top 10 VPN Service Reviews
https://**vpn**service.reviews/ ▾
Oct 4, 2016 - VPN Protocols. **PPTP** - A fast, easy-to-use protocol. L2TP/IPsec - A good choice if **OpenVPN** isn't supported by your device and security is top priority. **OpenVPN** - Recommended protocol for desktops. Chameleon - Great for VPN users being blocked in countries, or if you are experiencing bandwidth throttling.



chrome.google.com
View reputation details and comments

Your activity score is now **0**. Keep on rating to reach **bronze** level!

Trustworthiness
My Rating: click the bar to rate

Community Ratings
Excellent

Confidence: ●●●●●
Reasons: Good site, Online trackin, Other

Child Safety
My Rating: click the bar to rate

Community Ratings
Excellent

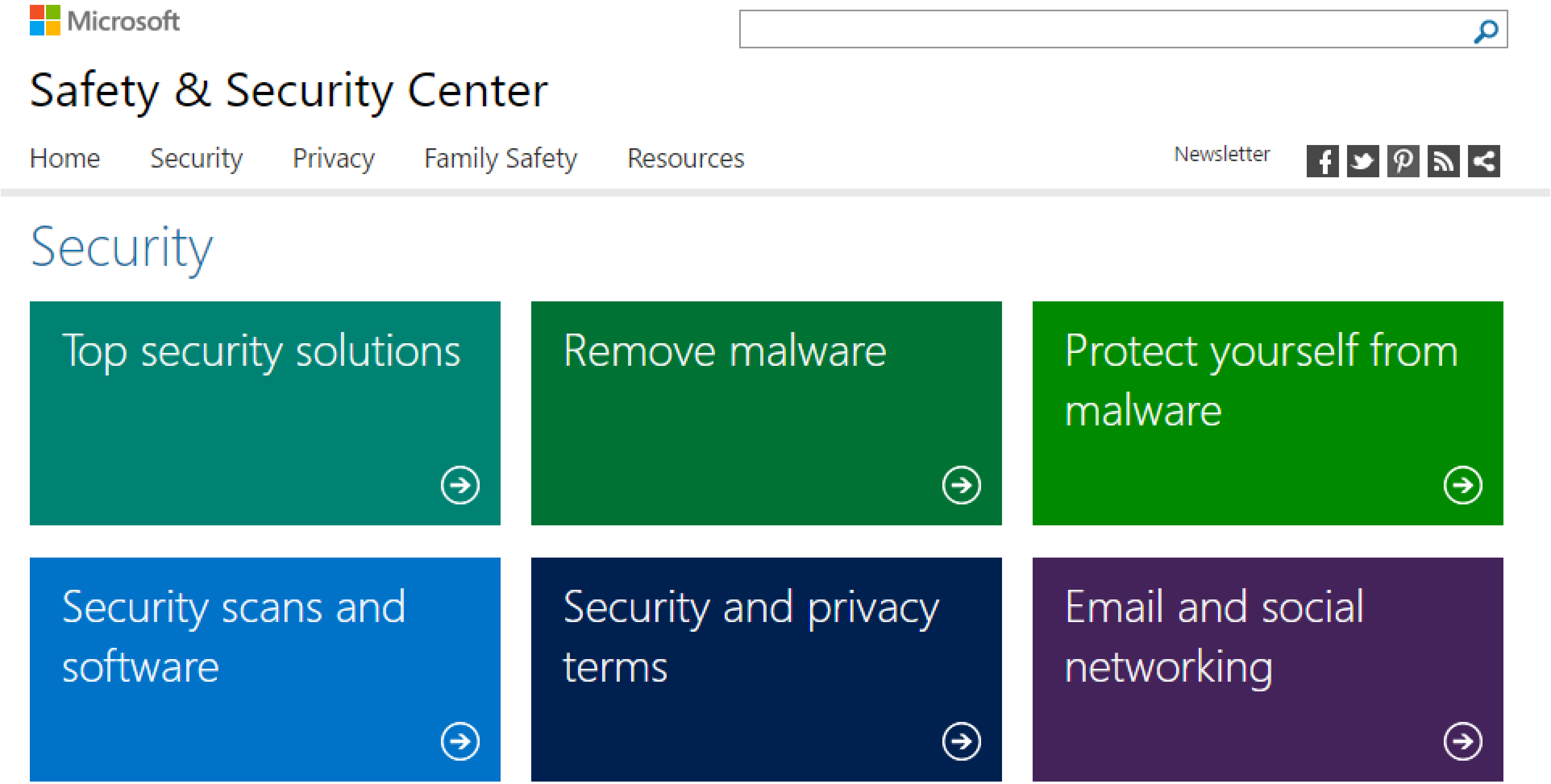
Confidence: ●●●●●
Reasons: Only for kids

WOT is now available for Android!

What Should You Do?

- Use the security information available on the Web
- You can search for virtually any security challenge / problem
- If you don’t like the first answers you get, refine your query
- As an example, Microsoft offers a Safety & Security Center
- Follow Tech news for new info about challenges / solutions
- Share questions (and solutions) with LCACE members
- Consider using a Chromebook / tablet as your laptop?

https://www.microsoft.com/en-us/safety/pc-security/default.aspx



Microsoft

Safety & Security Center

Home Security Privacy Family Safety Resources

Newsletter

Security

Top security solutions

Remove malware

Protect yourself from malware

Security scans and software

Security and privacy terms

Email and social networking

Privacy

- Adjust all Win 10 Settings for privacy
- Adjust privacy settings on every browser
- Install Ghostery or Disconnect as browser extension
- Use Duck, Duck Go as your search engine
- Install a Virtual Private Network (VPN)
- Use temporary or alias email addresses
- https://medium.freecodecamp.com/tor-signal-and-beyond-a-law-abiding-citizens-guide-to-privacy-1a593f2104c3#.be1pgqpr6