

CYBERSECURITY FUNDAMENTALS

CYBERSECURITY: HOW TO BECOME A HUMAN FIREWALL



Hartford Foundation

FOR PUBLIC GIVING

ABOUT COMMUNITY IT

*100% Employee
Owned*

*Advancing mission
through the effective
use of technology.*



Channel Futures.
Leading **Channel Partners** Forward

MSP 501
2021 WINNER

PRESENTER



Matthew Eshleman
CTO

AGENDA

Cybersecurity
Landscape



Human
Firewall



Putting it into
Action

CYBERSECURITY LANDSCAPE



Persistent and ongoing brute force attacks on identities



Sophisticated spearphishing



Organizations targeted because of the work they do



Attacks targeting vendors

CYBERSECURITY LANDSCAPE



New security tools available to combat new threat types.



Organization's starting to ask about where to start in improving their cybersecurity.



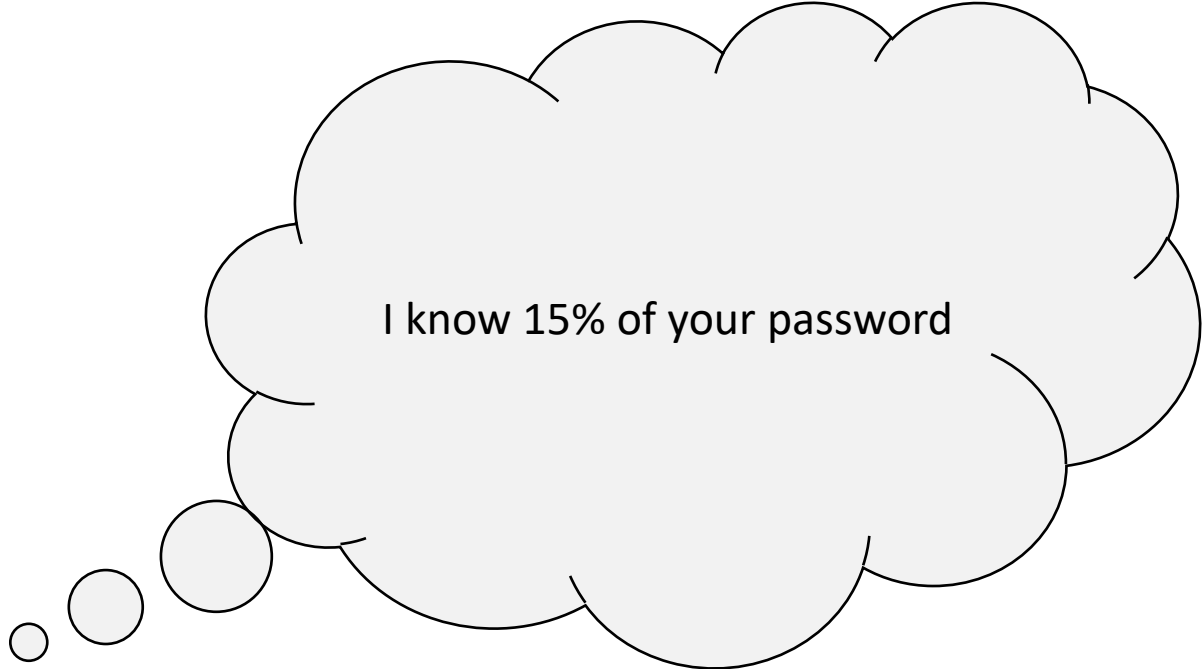
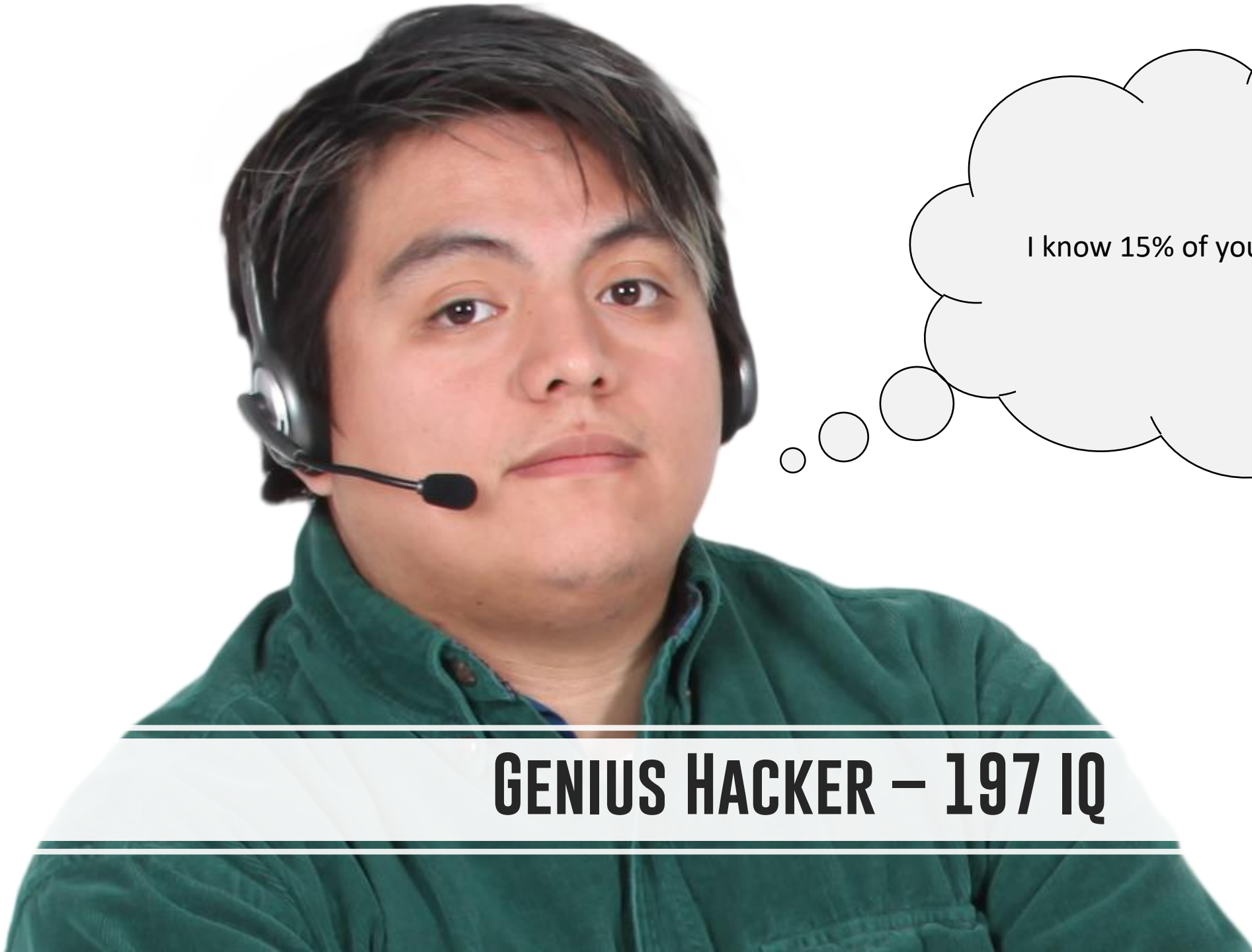
68% of Nonprofits don't have an Incident Response Plan



Breach response for a small to medium business is \$149,000

QUESTION

- How confident do you feel in your knowledge about Cybersecurity?
 - Very Confident
 - Confident
 - Somewhat Confident
 - Not at all Confident



GENIUS HACKER – 197 IQ

CYBERSECURITY - ADVERSARIES

FANCY BEAR



CYBERSECURITY OVERVIEW

It's good to talk openly
about cybersecurity

Share your story and
learn!

Your experience will
help someone else

CYBERSECURITY VULNERABILITY



- Supply Chain
- Staff at non-profits considered soft targets
- You may not consider your security important, but what about your donor list, board members, partners?

**CONTEMPORARY
ATTACK
EXAMPLES**

Email Phishing

Malware

Social
Engineering

Question (multiple choice)

- Have you experienced
 - Phishing emails
 - Virus / Malware / Ransomware
 - Social engineering

PHISHING

Common
attempts

How to identify

How to respond

From: OnlineInvoices Inc All Rights Reserved. <yourinvoice@medirestinc.com>

Sent: Thursday, March 8, 2018 12:23 PM

To: Matthew Eshleman <MEshleman@CommunityIT.com>

Subject: OnlineInvoices Automatic Service Notice

Online invoices
easy online billing

Invoice Notification

Good Day,

The following payment notification has been sent to you by OnlineInvoices on behalf of Pioneer Credit Recovery. Please click the button below to view your details

View Invoice

<http://corpcatererscleveland.com/?24=UCPAUBYKV1CQUuQZCQi>

\$4,260.00

Invoice Id Number15067557933



[About OnlineInvoices](#) | [Contact Us](#) | [Terms](#) | [Privacy Policy](#)

2018 OnlineInvoices.
Izam Inc. , 2715 Center Road , Suite 400, Wilmington, DE 19705

Email Preview - New device detected




From: alerts@devices-wellsfargo.com
Reply-to: alerts@devices-wellsfargo.com
Subject: New device detected


 [Send me a test email](#)
 [Toggle red flags](#)

WELLS FARGO

New Device Detected...

 [Dear customer,](#)

Click on the link below to update your devices.

 [Confirm your New Device](#)





To...

Joseph Weaver <jweavercpa@hotmail.com>

Cc...

Subject

RE: How Are You Doing?

From: Joseph Weaver <jweavercpa@sbcglobal.net>

PHISHING

1

Look at the email

2

Check for red
flags

3

Ask someone or
forward to your IT
support provider

MALWARE

Email
attachments

Malvertising

Spread via
networks



Lon Ryall

4:27 PM

Invoice INV-000993 from Property Lagoon Limited for Gleneagles Equestrian Centre

To: [redacted]



Invoice INV-000993.7z
3.48 KB

Malicious attachment

Dear customer,

Here's invoice INV-000993 for USD 502.52.

T <http://allsexfinder.com/inv-00022.7z>
Click or tap to follow link.

2.52 is due on 9 Sept 2017.

Malicious link

[View your bill online](#)

From your online bill you can print a PDF, export a CSV, or create a free login and view your outstanding bills.

If you have any questions, please let us know.

Thanks,

Lon Ryall
Property Lagoon Limited

File

Home

Insert

Design

Layout

References

Mailings

Review

View

Developer

Help



Paste



Clipboard

Arial

24

B

I

U

abc

X₂

X²

A

A

ab

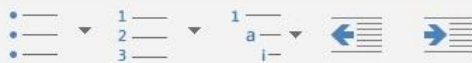
A

Aa

A

A

Font



Paragraph

AaBbCcDd

AaBbCcDd

Aa

Normal

No Spac...

He

Styles



SECURITY WARNING Macros have been disabled.

Enable Content



SECURE INVOICE



URGENT: Payment Overdue!!!

This document has been encrypted to protect your sensitive data

Please click "Enable Content" to view the invoice

This file is **100% virus-free**

NO VIRUSES NO SPYWARE NO ADWARE

ASADA issues 12,000 pages of evidence against 34 Essendon players

October 17, 2014 - 5:35PM

7 reading now

 Read later



Jon Pierik

Sports writer with The Age

[View more articles from Jon Pierik](#)

 [Follow Jon on Twitter](#)

 [Email Jon](#)

malvertisement 

Advertisement



Get \$100 in free ads

[Start now >](#)



Microsoft

 Tweet 3

 Recommend 2

 Share 1

 Share

 submit

 [Email article](#)

 [Print](#)

 [Reprints & permissions](#)

The 34 Essendon players re-issued with show-cause notices have been given 350 pages of evidence alleging they were administered a banned peptide during the club's 2012 supplements program.

Most popular

1 AFL trade and free





Dear Samsung SM-G930V user,

Wednesday, December 19, 2018

Congratulations Samsung SM-G930V user! You are one of the 10 users we personally selected to receive a \$250 Costco Gift Card!

OK

Costco Gift Card!

ACT NOW! 9 other Samsung users have received this invitation with only 5 prizes to be won.

You have **2 minutes 47 seconds** to answer the questions before someone else takes your spot. Good luck!

Question 1 of 4: Are you a regular Costco customer?

YES

```

0x0041ba35      align      8
aOutputs:
0x0041ba38      db         "Outputs", 0                ; DATA XREF=0x41b9ec
aEternalblueout:
0x0041ba40      db         "Eternalblue.Outputs", 0        ; DATA XREF=0x41b9e8
aShellcodebuffe:
0x0041ba54      db         "ShellcodeBuffer", 0           ; DATA XREF=0x41b810
aEternalblue:
0x0041ba64      db         "Eternalblue", 0               ; DATA XREF=0x41b974, 0x41b9f4
aEternalblueinp_41ba70: // aEternalblueinp
0x0041ba70      db         "Eternalblue__Inputs", 0        ; DATA XREF=0x41b970
aInputs:
0x0041ba84      db         "Inputs", 0                   ; DATA XREF=0x41b96c
0x0041ba8b      align      4
aEternalblueinp:
0x0041ba8c      db         "Eternalblue.Inputs", 0         ; DATA XREF=0x41b968
0x0041ba9f      align      32
aWindows7:
0x0041baa0      db         "Windows 7", 0                 ; DATA XREF=0x41e14c
0x0041baaa      align      4
aWindowsServer2_41baac: // aWindowsServer2
0x0041baac      db         "Windows Server 2008 R2", 0     ; DATA XREF=0x41e138
0x0041bac3      align      4
aWindowsServerR:
0x0041bac4      db         "Windows Server (R) 2008", 0    ; DATA XREF=0x41e124
aWindowsVista:
0x0041badc      db         "Windows Vista", 0             ; DATA XREF=0x41e110
0x0041baea      align      4
aWindowsServer2_41baec: // aWindowsServer2
0x0041baec      db         "Windows Server 2003 R2 3790", 0 ; DATA XREF=0x41e0fc
aWindowsServer2:
0x0041bb08      db         "Windows Server 2003 3790", 0  ; DATA XREF=0x41e0e8
0x0041bb21      align      4
aWindowsXp3790:
0x0041bb24      db         "Windows XP 3790", 0           ; DATA XREF=0x41e0d4
aWindows51:
0x0041bb34      db         "Windows 5.1", 0               ; DATA XREF=0x41e0c0
0x0041bb40      db 0x58 ; 'X'                            ; DATA XREF=sub_402d5f+209
0x0041bb41      db 0x50 ; 'P'
0x0041bb42      db 0x00 ; '.'

```


MALWARE

1

Have antivirus
and web filtering

2

Think before you
click (or call)

3

Ensure systems
are patched

SOCIAL ENGINEERING

Confidence
Scheme

Exploits trust

Sense of urgency


Email Login - Windows Internet Explorer

http://landmarks.com.mx/images/dropbox/9f6e6fc600e81cb59b74e50c82d84d3a/


Favorites Suggested Sites Web Slice Gallery

Email Login

Home RSS Print Page Safety Tools



Dropbox. Your stuff, anywhere.



To view the shared document, you are required to Login with your email address below:

Gmail **AOL** **Windows Live**

YAHOO! **Other emails**

Email Address:

Email Password:

Sign in



WARNING!

COMPUTER MAY BE AT RISK:

855-486-1800

Emergency Tech Support call immediately

Your system may have found (2) viruses that pose a serious threat

Rootkit.Sirefef.Spy ./ Trojan.FakeAV-Download

Your personal and financial information

may not be secured.

Call us now for support

855-486-1800

TECH SUPPORT

LogMeIn Rescue

Your desktop is being remote controlled by [redacted]

9:22 AM Connecting...

9:22 AM Connected. A support representative will be with you shortly.

9:23 AM Support session established with [redacted].

9:23 AM [redacted] restarting application as Windows system service

9:23 AM Connecting...

9:23 AM Connected. A support representative will be with you shortly.

9:23 AM Connection closed. Attempting reconnection...

9:23 AM Application running as Windows system service

9:23 AM Support session established with [redacted].

9:23 AM You have granted full permission to [redacted]. To revoke, click the red X on the toolbar or press Pause/Break on the keyboard.

9:23 AM Remote Control started by [redacted].

Type here and press Enter to send

SOCIAL ENGINEERING

1

Trick you into installing software

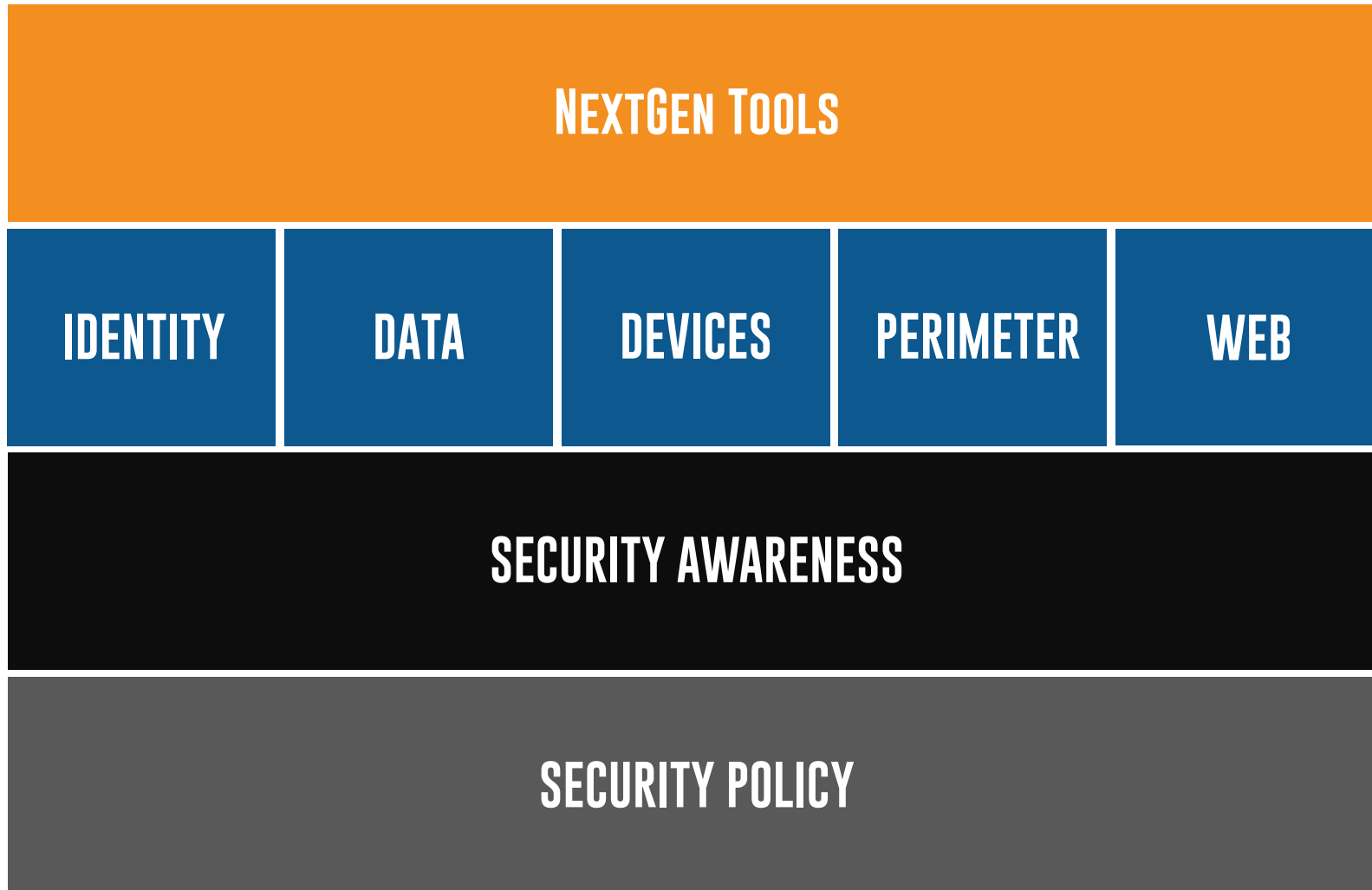
2

Trick you into entering credentials

3

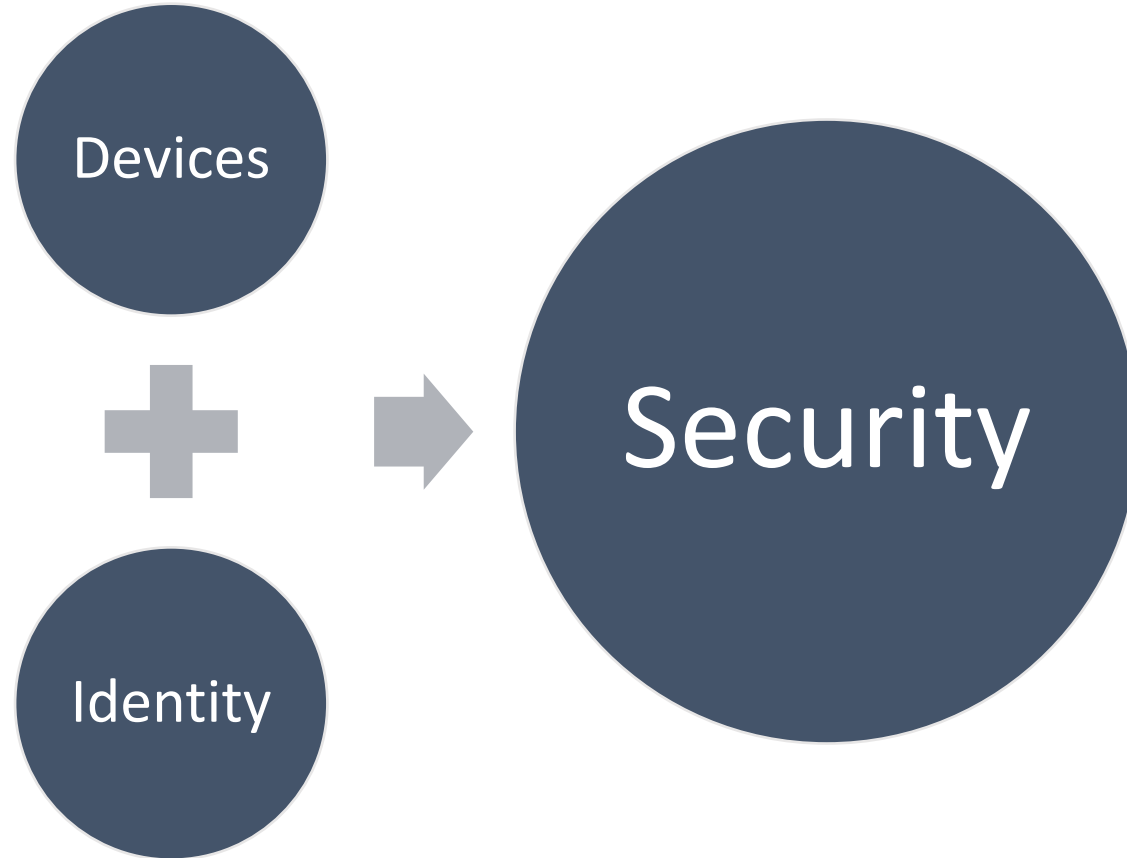
Trick you into calling for "support"

OUR APPROACH TO CYBERSECURITY



HUMAN FIREWALL





HUMAN FIREWALL



You're capable of protecting your information

- Inventory
- Backup your data

HUMAN FIREWALL



Patch and Update

- OS
- Firmware
- All devices
- Monthly

HUMAN FIREWALL



Enable and use
Antivirus

- Only 40% effective
(but 40% is better
than 0%!)

HUMAN FIREWALL



- Audit access to your Cloud Systems
- Be aware and honest

HUMAN FIREWALL



See my
password
on the back
side

- Pick a good password
- Use a password Manager
- Enable MFA

**SECURITY NONEXPERTS' TOP
ONLINE SAFETY PRACTICES**

VS

**SECURITY EXPERTS' TOP
ONLINE SAFETY PRACTICES**

1. USE ANTIVIRUS
SOFTWARE



2. USE STRONG
PASSWORDS



3. CHANGE PASSWORDS
FREQUENTLY



4. ONLY VISIT WEBSITES
THEY KNOW



5. DON'T SHARE
PERSONAL INFORMATION



1. INSTALL SOFTWARE
UPDATES



2. USE UNIQUE
PASSWORDS



3. USE TWO-FACTOR
AUTHENTICATION



4. USE STRONG
PASSWORDS



5. USE A PASSWORD
MANAGER

SECURITY CHECKLIST

1. Backups
2. Updates
3. Antivirus
4. Audit Systems
5. Strong Passwords with MFA

PUTTING IT INTO ACTION

Inventory systems

- Desktop
- Email
- Cloud Services
- Photos

Backup

- 2 locations
- You have control

PUTTING IT INTO ACTION

Update your systems

- Operating System (Windows, Mac, iOS, Android)
- BIOS and Firmware Updates Quarterly
- Reboot weekly

PUTTING IT INTO ACTION

Antivirus

- Windows Defender
- MacOS, XProtect

Web Filtering

- Cisco Umbrella
- Cloudflare

PUTTING IT INTO ACTION

Get a password manager

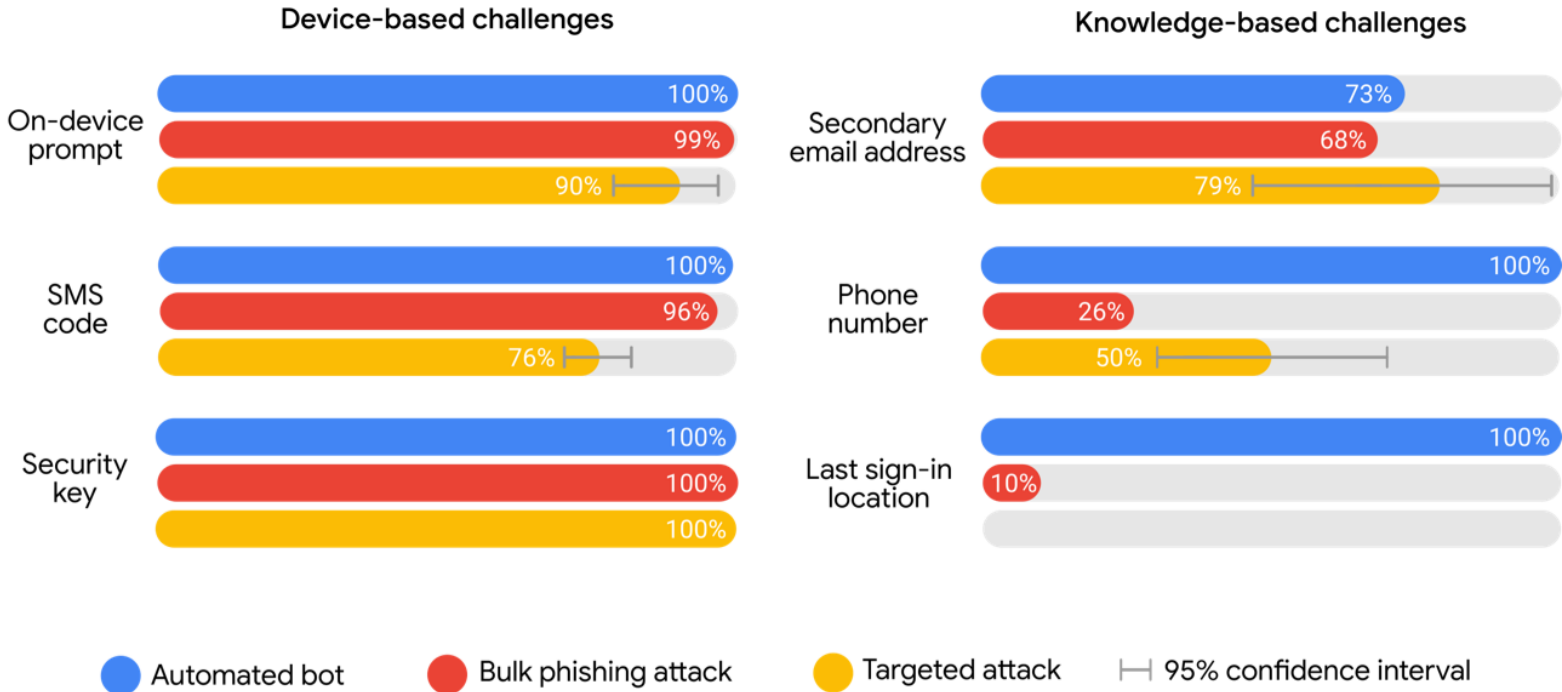
- LastPass
- Dashlane

Pick a strong password

- Passphrase
 - One for your computer, one for the password manager
- Here are some guides
 - <http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/>
 - <https://haveibeenpwned.com/Passwords>
- Enable MFA
 - [O365 MFA Enrollment Guide](#)
 - [Google Workspace MFA Guide](#)

MFA IS EFFECTIVE

Account takeover prevention rates, by challenge type



Pwned Passwords

Pwned Passwords are half a billion real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. [Read more about how HIBP protects the privacy of searched passwords.](#)



pwned?

Oh no — pwned!

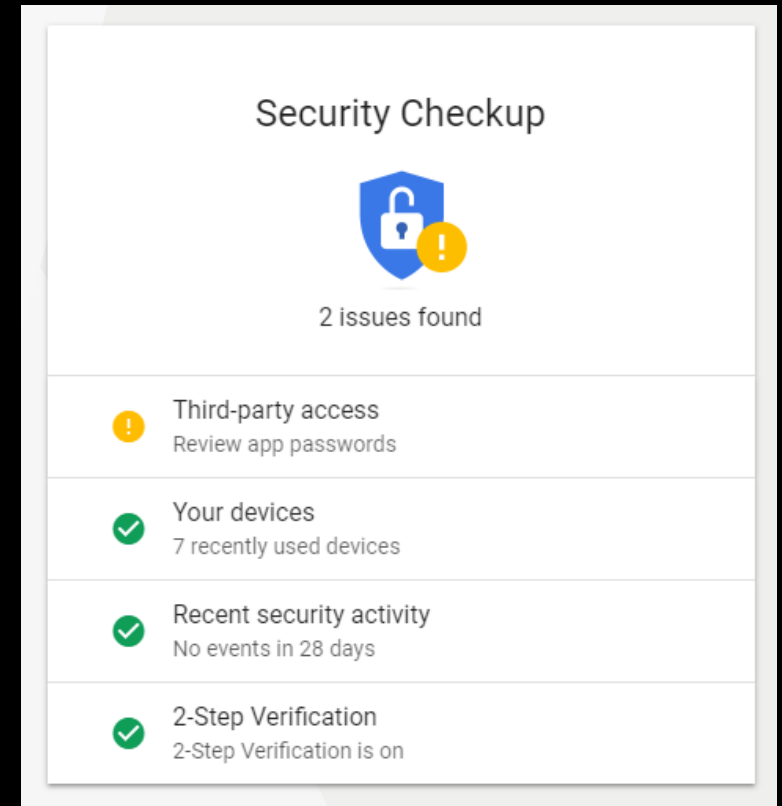
This password has been seen 7 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

SECURITY CHECK UP

Audit access to applications

- Facebook -
<https://www.facebook.com/help/799880743466869>
- Google -
<https://myaccount.google.com/intro/security-checkup?hl=en-US>
- LinkedIn -
<https://www.linkedin.com/psettings/>



MOVING FORWARD

Security can be daunting, but it doesn't need to be overwhelming

MOVING FORWARD

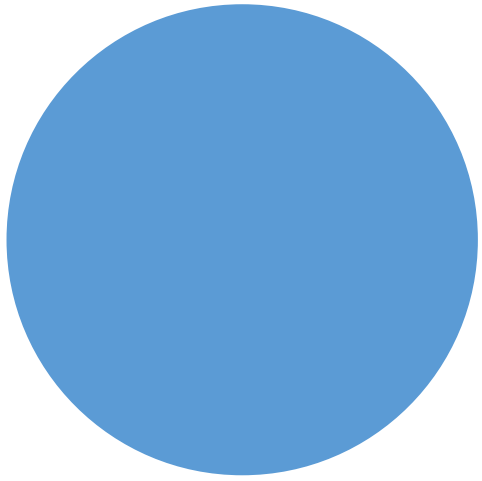
Steps you can take

- Inventory and backup your data
- Update your computer (OS and Firmware)
- Make sure AV is installed
- Select a good password
 - Use a password manager
 - Turn on MFA
- Review System access and remove extra/unnecessary applications
- Schedule time for security

SCHEDULE TIME FOR SECURITY



- Set a reminder for yourself
 - one week from today
- Have an accountability partner
 - monthly check in



QA



RESOURCES

- Community IT Webinar – <https://www.communityit.com>
- Stop Think Connect – <https://www.stopthinkconnect.org>