James M.T. Morrison

Distinguished Technologist—Cyber Security
Office of the North America CTO
Hewlett Packard Enterprise

Director of Business Development
Shyield LLC

James Morrison joined Hewlett Packard Enterprise (HPE) in December 2019 from the Federal Bureau of Investigation (FBI) as a Distinguished Technologist - Cyber Security in the office of the North America CTO.

James spent 22 years with the FBI as a Senior Computer Scientist, focused on cyber security. He worked on numerous national security and criminal intrusion investigations, as an active Cyber Security Expert, identifying security vulnerabilities and implementing solutions. He was a Regional Program Manager for the FBI Computer Science program and Adjunct Faculty Member for the FBI, teaching multiple classes at Quantico and internationally.

Succeeding in the idea economy requires IT to evolve from a provider of basic business support into an engine of value creation. HPE's GreenLake Private Cloud is the cloud that comes to you with the security & flexibility of Traditional IT, while delivering public cloud economics - accelerating both digital and business transformation.

Phone (281) 889.0565 **E** James.M.Morrison@HPE.com **W** hpe.com

Hewlett Packard Enterprise

Shyield

Computer Threats

James M.T. Morrison
FBI Computer Scientist (Retired)

James Morrison and Fidelity investments are not Affiliated

Introduction

James M.T. Morrison (aka Uglymother)

- Cybersecurity Technologist with HPE
- 22 Years of Experience with the FBI
- 8 Years US Air Force
- 31+ Years in the IT field
- BS in Computer Engineering, MBA Technical Management
- GCED, GREM, GCIA, GCIH, GCFA, GCFE, GPEN, GWAPT, GMOB, A+, Net+

Introduction

Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems

— Kevin Mitnick —

AZ QUOTES

Headlines

Beware of Robocalls, Texts and Emails Promising COVID-19 Cures or Fast Stimulus Payments

Coronavirus scams spreading as fraudsters follow the headlines

by John Waggoner and Andy Markowitz, **AARP**, Updated August 31, 2020 | Comments: 7

The latest ways identity thieves are targeting you — and what to do if you are a victim

PUBLISHED THU, FEB 27 2020•10:18 AM EST | UPDATED THU, FEB 27 2020•10:36 AM EST

Scott Steinberg, special to CNBC.com

Covid Numbers

1. Unsecured Remote Desktops Rose by 40%
2. RDP Brute Force Attacks Rose 400% in March/April
3. E-Mail scams related to COVID rose 667% in March
4. Users are now three times more likely to click on pandemic related phishing scams
5. There are now 4.8 billion Covid-19 pages
6. Tens of Thousands New Covid Domains created daily
7. 90% of newly created Coronavirus domains are scam related
8. More than 530,000 Zoom Accounts Sold on the Dark Web
9. 2000% Increase in Malicious Files with Zoom in Name
10. Covid-19 Drives a 72% to 105% Ransomware Spike

Global Cybercrime Damage Costs:

- **$6 Trillion USD a Year. ***
- **$500 Billion a Month.**
- **$115.4 Billion a Week.**
- **$16.4 Billion a Day.**
- **$684.9 Million an Hour.**
- **$11.4 Million a Minute.**
- **$190,000 a Second.**

ALL FIGURES ARE PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

Social Attacks

- Phishing
- Watering Hole
- Whaling
- Pretexting
- Baiting

Phishing

- Messages are composed to attract the user's attention.
- Phishing messages aimed at gathering a user's information convey a sense of urgency.
- Attackers leverage shortened URL or embedded links to redirect victims to a malicious domain
- Phishing email messages have a deceptive subject line to entice the recipient to believe that the email has come from a trusted source.

Combating Social Attacks

- Slow down.
- Research the facts.
- Don’t let a link be in control of where you land.
- Email hijacking is rampant.
- Beware of any download.
- Foreign offers are fake

Combating Social Attacks

Phishing Statistics

30% of phishing messages are opened by targeted users, and 12% of those users click on the malicious attachment or link.

keepnet LABS

What Can Happen?

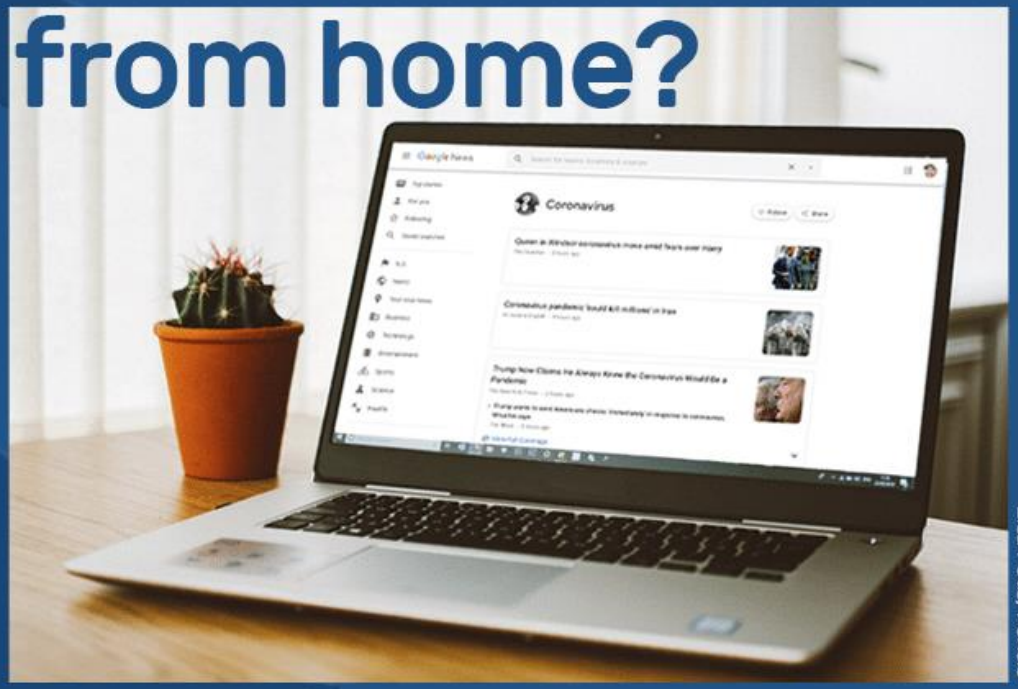
- **ACCOUNT TAKEOVER**
  - A form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials.
- **RANSOMWARE**
  - A type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
- **KEYSTROKE LOGGING**
  - A type of malicious malware (commonly) that records the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored.

Exploit the Home User

Working from home?

Be careful what you click on ...

Cybercriminals are out there!



Lisa Fotis/Pexels

CISA
CYBER+INFRASTRUCTURE

How Often Are Home Networks Attacked

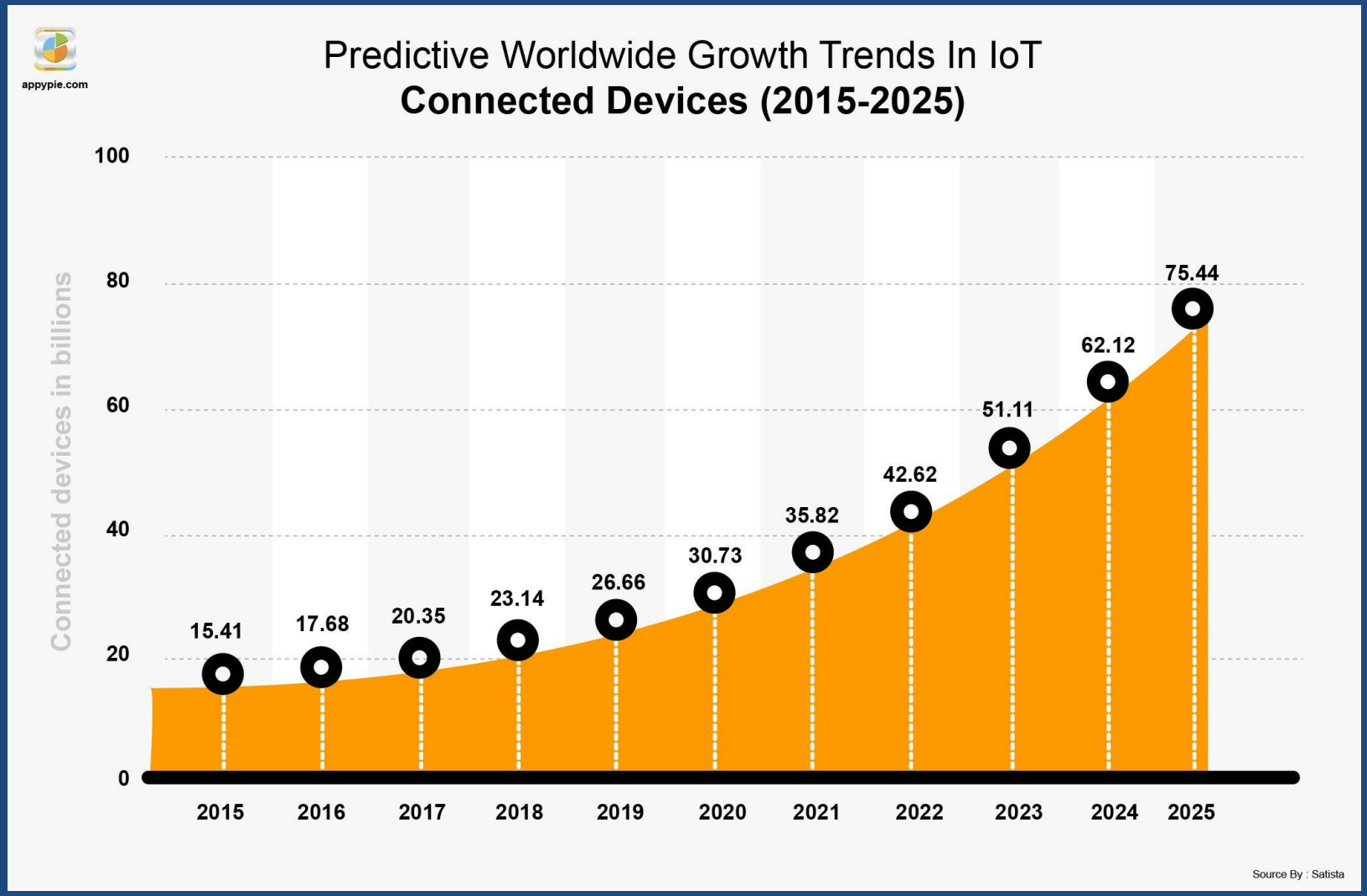
Cybersecurity report: Average household hit with 104 threats each month

- Nearly all of the respondents (95%) underestimated the monthly cyberattack volume targeting their households. On average, respondents believed they faced 12 attacks monthly
- Households … have an average of 12 devices in their home, although "high-end users" have up to 33 devices, per the report
- 64% simultaneously said they also shared passwords with family members and friends

Tips for Working from Home

- Lock your devices
- Secure your router's password
- Personal devices vs. work devices
  - Do what you can to keep personal devices separate from your work devices.
- The latest security news
  - Dedicate some time on a regular basis to read up on the latest security news to stay in the know about recent vulnerabilities, attacks and breaches.
- Use a VPN and avoid public Wi-Fi networks
- Prioritize your mental health

Internet of Things (IoT)



Cell Phones


LE VPN
INTERNET BY YOUR OWN RULES
SMART PHONE SECURITY THREATS
Downloadable Applications Threats:
Malware
Spyware
Privacy
Zero Day Vulnerabilities
General Cyber Security Threats:
Phishing
Social Engineering
Drive By Downloads
Browser Flaws
OS Flaws
Data Storage
Network and WiFi Security Threats:
Network Exploits
WiFi Sniffing
Cross-Platform Attacks
BOYD
Physical Threats:
Loss/Theft
1
2
3
4

USB Threats

ARE YOU PREPARED FOR USB BASED ATTACKS?

If your business hasn't taken steps to protect against USB-based attacks, your network security plan is not complete.

Passwords Facts

1. 40% of people store privileged and administrative passwords in a Word document, spreadsheet, or Notes.
2. When people are asked to include a number in a password, the majority simply add a “1” or a “2” at the end.
3. Two-thirds of people use no more than two passwords for all their online accounts.

Passwords

What is the Most Common Password in the World?

Passwords

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

Passwords – Best Practices

- Do not use the same password for all websites
- Use Password Managers
  - Cloud-Based or Apps are Most Common
- Longer is Better (Add 4 to the min password)
- Alter your Password Patterns
  - Don’t Capitalize First Letter
  - Don’t End with Numbers
- Use Passphrases instead of Passwords

Passwords – Who Cares

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper Case	Mixed Lower, Upper Case and Numbers	Mixed Lower, Upper Case, Numbers, and Symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Common Scams

- Threatening calls from the IRS/FBI/Social Security.
- Technical support calls.
- Fake charity appeals.
- Lottery scams.
- Family members in peril.
- Bank fraud calls.
- Insurance, health care and debt scams.
- Website password requests.
- Fake customer requests.
- Other urgent requests.

Don't say anything online that you wouldn't want plastered on a billboard with your face on it.

– Erin Bury

Social Media ”Rules”

1. Know What You Have Posted About Yourself
2. Don’t trust that a message really is from whom it says it’s from
3. Assume that everything you put on a social networking site is permanent.
4. Be selective about who you accept as a friend on a social network.

Combating Online Harassment

1. Identify your crime
2. Disengage
3. Talk to your ”Inner Circle”
4. Document
5. Contact Law Enforcement
6. Protect Yourself (Lock things down)

Relationships Fraud

"CATFISH" Rules

1. Speak with them
2. Video Chat with them
3. Meet them in a public location with backup
4. $$ Should never be a Topic

Internet Fraud

Identity Theft - Statistics

- In 2019, 14.4 million consumers became victims of identity fraud — that's about 1 in 15 people
- Overall, 33 percent of U.S. adults have experienced identity theft, which is more than twice the global average
- More than one in four older adults, aged 55 and over, have experienced identity theft
- One in five victims of identity theft have experienced it more than once
- Over 1 million children in the U.S. were victims of identity theft in 2017, costing families $540 million in out-of-pocket expenses
- There's a new victim of identity theft every 2 seconds
- Children are 51 times more likely to be a victim of identity theft than adults
- Identity theft is the most common consequence of a data breach, occurring 65% of the time
- There were 164 million exposed records in 2019, and data breaches increased by 17%
- Consumers lost more than $1.9 billion to identity theft and fraud in 2019

How to Protect Identity

Equifax data breach: How to freeze your credit

Alia E. Dastagir, USA TODAY Published 11:52 a.m. ET Sept. 13, 2017 | **Updated 3:29 p.m. ET Sept. 13, 2017**

To place a freeze on your credit reports, you need to call or visit the websites of the credit reporting companies. There are three big ones — Equifax, Experian and TransUnion.
Litan recommends freezing your credit at all three.

Equifax / Experian / TransUnion
(Visit Their Websites)

Protect, Update and Backup

Your Internet browser, operating system, anti-virus, and other programs should be updated regularly. Use an external or cloudbased backup system to save photos and documents.

Securing the Network (Individual)

1. Purchase an Internet Security Product and Keep it updated
2. Backup your pictures and documents – do not leave them in your email
3. Do not click on Links and Attachments unless you are absolutely sure where it came from
4. Use Two-factor Authentication everyplace you can
5. Password Management
6. Consider an Identity Protection Service
7. Know that e-mail is not trustworthy

Public Wi-Fi Safety

- Passersby can look over your shoulder onto your laptop screen (Shoulder Surfing)
- Passersby can eavesdrop on your phone conversations
- WiFi networks can be insecure (They should always be considered this)
- The chance of leaving a device in a place where it might easily be stolen increases.

Internet Crime Complaint Center (www.IC3.gov)

Or

Call: 1-800-CALL-FBI

Questions??

James Morrison

FBI (Retired)

GCED, GFCE, GCFA, GPEN, GCIA, GCIH, GREM, GMOB
CEH, MBA, MA

mail@txcyberguy.com