Cybersecurity: Week 2 Securing Our "Things"

Blake Carver
Senior Systems Administrator, LYRASIS
April 2021
Cybersecurity Training for Libraries
Week #2

1

This project was supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred.

2

Today's Schedule

10:00 – 10:20 Welcome & course housekeeping
10:20 – 10:45 Training
10:45 – 10:50 Break
10:50 – 11:25 Training
11:25 – 11:30 Wrap up

3

Series Housekeeping - Outline

- **Week One – Welcome – Explanations of why and what's wrong**
- Touch on some privacy issues.
- Why are libraries, and all of us, targets?
- Why is security important?
- Professionals and Incentives, big money.
- What are they after and where are they working?
- Passwords

- **Week Two – Securing our things**
- Passwords
- What things do we have to secure?
- Hardware, software, etc
- How do things actually get infected? How can we spot it?
- Email, phishing, browsers, VPNs, Tor,
- desktop, mobile, everything else.

- **Week Three - Making Your Library Defensible & Resilient**
- What and why of things around the library
- Hardware, networks, ransomware

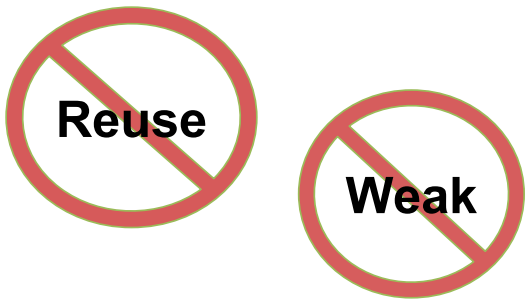
- **Week Four – Wrapping It All Up**
- Training, planning, vendors
- Websites
- Checklists and specific steps to take next.

4

The Importance Of Passwords For You & Your Library

5

Passwords



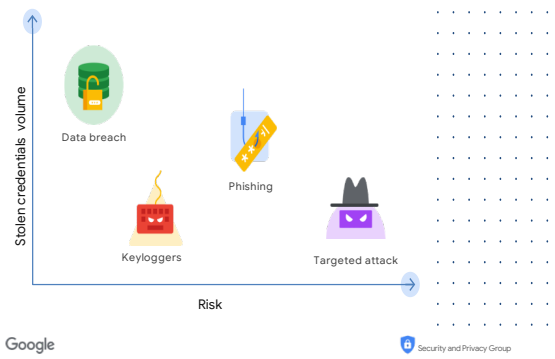
6

7

How Did They Get My Password?

Guessed
Password Reset
Stolen Mobile Device
Phishing
Trojans/Virus/Malware
API Exploitation
Third Party App Exploitation
Website Breach

8



9

Stolen credential origin takeaways

The black market fuels account compromise

Password reuse is the largest source of compromise

Phishing pose significant risk

Google

Security and Privacy Group

10

people respond to policies, *perversely*

ZAQ!@#$
P@5sw0rd1!

Passwords

11

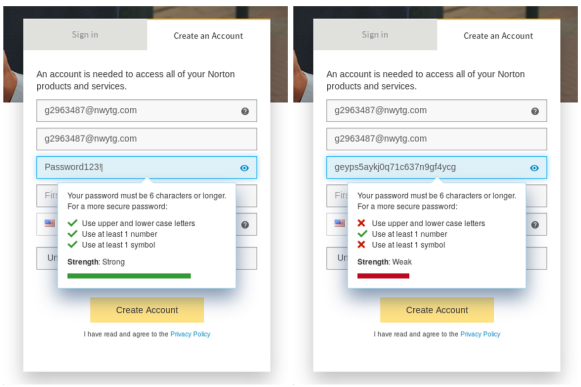
49% of workers, when forced to update their password, reuse the same one with just a minor change

Graham Cluley
11:15 am, December 11, 2019

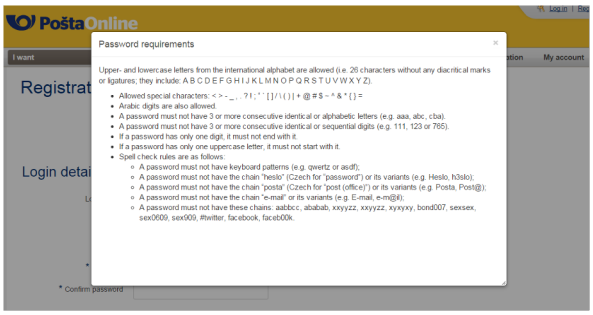
For instance, not only did 72% of users admit that they reused the same passwords in their personal life, but also 49% admitted that when forced to update their passwords in the workplace they reused the same one with a minor change.

Furthermore, many users were clearly relying upon their puny human memory to remember passwords (42% in the office, 35% in their personal lives) rather than something more reliable. This, no doubt, feeds users' tendency to choose weak, easy-to-crack passwords as well as reusing old passwords or making minor changes to existing ones.

12


Sign in
Create an Account
An account is needed to access all of your Norton products and services.
g2963487@nwytg.com
g2963487@nwytg.com
Password123|
Your password must be 6 characters or longer. For a more secure password:
Use upper and lower case letters
Use at least 1 number
Use at least 1 symbol
Strength: Strong
Create Account
I have read and agree to the Privacy Policy
Sign in
Create an Account
An account is needed to access all of your Norton products and services.
g2963487@nwytg.com
g2963487@nwytg.com
geyps5aykj0q71c637n9gf4ycg
Your password must be 6 characters or longer. For a more secure password:
Use upper and lower case letters
Use at least 1 number
Use at least 1 symbol
Strength: Weak
Create Account
I have read and agree to the Privacy Policy

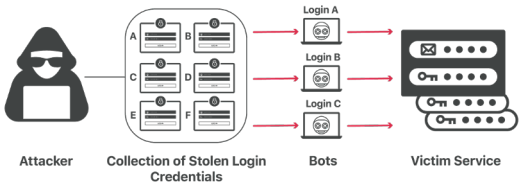
13


PoštaOnline
Password requirements
Upper- and lowercase letters from the international alphabet are allowed (i.e. 26 characters without any diacritical marks or ligatures; they include: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z).
Allowed special characters: < > - _ , . ? ! ; " ' [ ] / \ ( ) | + @ # $ ~ ^ & * { } =
Arabic digits are also allowed.
A password must not have 3 or more consecutive identical or alphabetic letters (e.g. aaa, abc, cba).
A password must not have 3 or more consecutive identical or sequential digits (e.g. 111, 123 or 765).
If a password has only one digit, it must not end with it.
If a password has only one uppercase letter, it must not start with it.
Spell check rules are as follows:
A password must not have keyboard patterns (e.g. qwertz or asdf);
A password must not have the chain "heslo" (Czech for "password") or its variants (e.g. Heslo, h3slo);
A password must not have the chain "posta" (Czech for "post (office)") or its variants (e.g. Posta, Post@);
A password must not have the chain "e-mail" or its variants (e.g. E-mail, e-m@il);
A password must not have these chains: aabbcc, ababab, xxyyzz, xxyyzz, xyxyxy, bond007, sexsex, sex0609, sex909, #twitter, facebook, facebOOk.

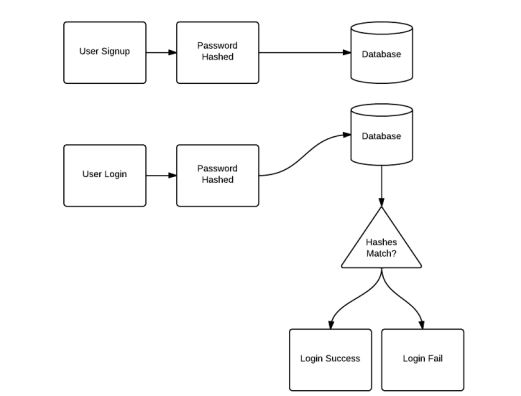
14


Set password
Password too long

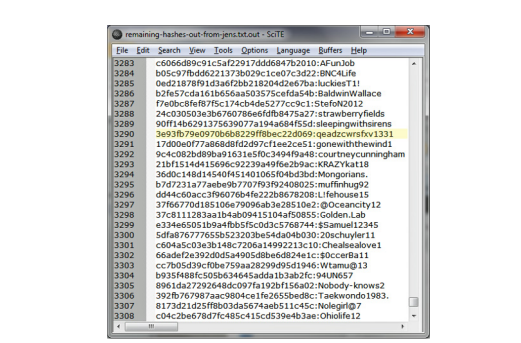
15


Login A
Login B
Login C
A
B
C
D
E
F
Attacker
Collection of Stolen Login Credentials
Bots
Victim Service

16


User Signup
Password Hashed
Database
User Login
Password Hashed
Database
Hashes Match?
Login Success
Login Fail

17

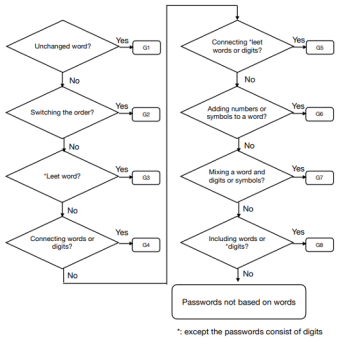

remaining-hashes-out-from-jens.txt.out - SciTE
File Edit Search View Tools Options Language Buffers Help
3283 c6066d89c91c5af22917ddd6847b2010:AFunJob
3284 b05c97fbdd6221373b029c1ce07c3d22:BNC4Life
3285 0ed21878f91d3a6f2bb218204d2e67ba:luckiesT1!
3286 b2fe57cda161b656aa503575cefda54b:BaldwinWallace
3287 f7e0bc8feff875c174cb4de5277cc9c1:StefoN2012
3288 24c030503e3b6760786e6fdfb8475a27:strawberryfields
3289 90ff14b629137563907 7a194a684f55d:sleepingwithsirens
3290 3e93fb79e09700b6b8229ff8bec22d069:qeadzcwrsfxv1331
3291 17d00e0f77a868d8fd2d97cf1ee2ce51:gonewiththewind1
3292 9c4c082bd89ba91631e5f0c3494f9a48:courtneycunningham
3293 21bf1514d415696c92239a49f6e2b9ac:KRAZYkat18
3294 36d0c148d14540f45140106 5f04bd3bd:Mongorians.
3295 b7d7231a77aebe9b7707f93f92408025:muffinhug92
3296 dd44c60acc3f96076b4fe222b8678208:L1fehouse15
3297 3766770d185106e79096ab3e28510e2:@Oceancity12
3298 37c8111283aa1b4ab09415104af50855:Golden.Lab
3299 e334e65051b9a4fbb5f5c0d3c5768744:$Samuel12345
3300 5dfa876777655b523203be54da04b030:2Oschuyler11
3301 c604a5c03e3b148c7206a1499221 3c10:Chealsealove1
3302 66adef2e392d0d5a4905d8be6d824e1c:$0ccerBa11
3303 cc7b05d39cf0be759aa28299d95d1946:Wtamu@13
3304 b935f4b88c505b634645add a1b3ab2fc:94UN657
3305 8961da27292648dc097fa192bf156a02:Nobody-knows2
3306 392fb767987aac9804ce1fe2655bed8c:Taekwondo1983.
3307 8173d21d25ff8b03da5674aeb511c45c:Nolegirl@7
3308 c04c2be678d7fc485c415cd539e4b3ae:Ohiolife12

18

```
hashcat (v6.1.1) starting in benchmark mode...

CUDA API (CUDA 11.0)
====================
* Device #1: A100-PCIE-40GB, 40121/40537 MB, 108MCU
* Device #2: A100-PCIE-40GB, 40121/40537 MB, 108MCU
* Device #3: A100-PCIE-40GB, 40121/40537 MB, 108MCU
* Device #4: A100-PCIE-40GB, 40121/40537 MB, 108MCU

OpenCL API (OpenCL 1.2 CUDA 11.0.228) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #5: A100-PCIE-40GB, skipped
* Device #6: A100-PCIE-40GB, skipped
* Device #7: A100-PCIE-40GB, skipped
* Device #8: A100-PCIE-40GB, skipped

Benchmark relevant options:
===========================
* --optimized-kernel-enable

Hashmode: 3200 - bcrypt $2*$, Blowfish (Unix) (Iterations: 32)

Speed.#1.........:   140.8 kH/s (149.44ms) @ Accel:10 Loops:22 Thr:40 Vec:1
Speed.#2.........:   140.8 kH/s (149.41ms) @ Accel:10 Loops:22 Thr:40 Vec:1
Speed.#3.........:   140.8 kH/s (149.45ms) @ Accel:10 Loops:22 Thr:40 Vec:1
Speed.#4.........:   140.8 kH/s (149.54ms) @ Accel:10 Loops:22 Thr:40 Vec:1
Speed.#*.........:   563.2 kH/s

Started: Sat Oct  3 22:22:19 2020
Stopped: Sat Oct  3 22:22:39 2020
```

19

PCFG Cracker - Probabilistic Context Free Grammar (PCFG) Password Guess Generator



*: except the passwords consist of digits

20

- **Traditional Brute-Force Attack**: A dedicated, purpose-written software package generates all combinations of letters, numbers, and other characters such as punctuation and symbols, in progressively longer strings. It tries each one as the password on the account under attack. If it happens to generate a combination of characters that matches the password for the account under attack, that account is compromised.
- **Dictionary Attack**: A dedicated, purpose-written software package takes one word at a time from a list of dictionary words, and tries them as the password against the account under attack. Transformations can be applied to the dictionary words such as adding digits to them and substituting digits for letters.
- **Password Look-Up Attack**: Similar to a dictionary attack, but the word lists contain actual passwords. Automated software reads a password at a time from a huge list of passwords collected from data breaches.
- **Intelligent Password Look-Up Attack**: Like a password attack, but transformations of each password are tried as well as the "naked" password. The transformations emulate commonly used password tricks such as substituting vowels for digits.
- **API Attack**: Instead of trying to crack a user's account, these attacks use software to generate strings of characters they hope will match a user's key for an Application Programming Interface. If they can get access to the API they may be able to exploit it to exfiltrate sensitive information or intellectual copyright.

https://www.cloudsavvyit.com/7132/how-to-protect-your-organization-against-password-dictionary-attacks/

21

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{3})
m – Million (1,000,000 or 10^{6})
bn – Billion (1,000,000,000 or 10^{9})
tn – Trillion (1,000,000,000,000 or 10^{12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{18})

22

https://johnopdenakker.com/every-day-should-be-worldpasswordday/

23

Simple Things Make Strong Passwords (*Slow Them Down*)

- DO Make it as _l o n g_ as you can
- Do not reuse it on multiple sites
- Do not use numb3r5 1n pl@c3 of l3tt3rz
- Some Letters – UPPER and lower case
- Use some numbers
- Have a something else <>(*%$@!-+=)
- S P A C E S

24

Don't Test Your Memory

Anything dependent on memory doesn't scale

- Use a password manager
  - Bitwarden, LastPass, KeePass[X], 1Password, Dashlane..
- Use A Pass Phrase
- Nobody – *nobody* – is immune from getting hacked

25

Should You Change Your Passwords Every X # of Months?

- Email?
- Bank Account?
- Network? Server? Router?
- Facebook & Twitter?
- code4lib.org?
- ala.org?

26

Assume Your Password Will Be Stolen

Most of your passwords should be almost worthless. Some will be very important.

27

What Else Ya Got?

- Biometrics
- Hardware
- Your face
- Iris scans
- Voice files
- Your DNA
- Your voice
- 2 Factor Authentication
- Security Questions

...More Confusion ...More Work ...More Money

28

Here's Why [Insert Thing Here] Is Not a Password Killer

05 NOVEMBER 2018

Every single solution I've seen that claims to "solve the password problem" ***just adds another challenge in its place thus introducing a new set of problems.***

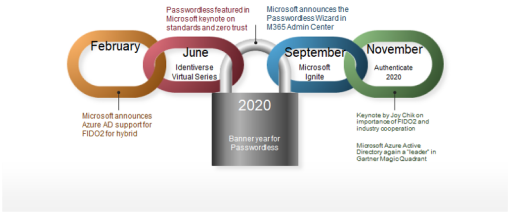
This is why [insert thing here] is not a password killer and why, for the foreseeable future, we're just going to have to continue getting better at the one authentication scheme that everyone knows how to use: passwords.

https://www.troyhunt.com/heres-why-insert-thing-here-is-not-a-password-killer/

29

Microsoft: Next steps for passwordless in 2021

Our team has been working hard this year to join these partners in making passwords a thing of the past. Along with new UX and APIs for managing FIDO2 security keys enabling customers to develop custom solutions and tools, we plan to release a converged registration portal in 2021, where all users can seamlessly manage passwordless credentials via the My Apps portal.



https://www.microsoft.com/security/blog/2020/12/17/a-breakthrough-year-for-passwordless-technology/

30

Securing The "Things"

31

"Things"

32

It's not about what's most secure…
it's about what the bad guys focus on

33

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS

*INTERNET OF SH*T —*

When coffee makers are demanding a ransom, you know IoT is screwed

Watch along as hacked machine grinds, beeps, and spews water.

DAN GOODIN - 9/26/2020, 10:58 AM

Additionally, this case also demonstrates one of the most concerning issues with modern IoT devices: **"The lifespan of a typical fridge is 17 years, how long do you think vendors will support software for its smart functionality?"** Sure, you can still use it even if it's not getting updates anymore, but with the pace of IoT explosion and bad attitude to support, we are creating an army of abandoned vulnerable devices that can be misused for nefarious purposes such as network breaches, data leaks, ransomware attack and DDoS.

https://arstechnica.com/information-technology/2020/09/how-hackers-turned-a-250-coffee-maker-into-a-ransom-machine/

34

Share of IoT infections has increased by 100%

IoT devices now make up 32.72% of the infected devices observed. Compared with 2019, the share occupied by IoT devices in the overall device breakdown has increased by 100%, from a previous share of 16.17%.

With the widespread proliferation of IoT devices, it is to be expected that the number of IoT infections will grow dramatically. As Figure 3 demonstrates, in 2020 this led to the increase of the share that IoT infections have in the overall device breakdown.

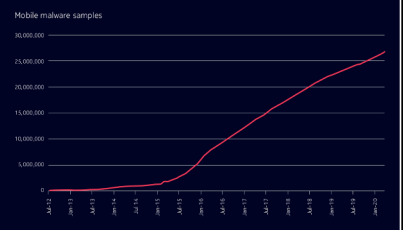
The rate of success in infecting IoT devices depends dramatically with the visibility of the devices to the internet. In networks where devices are routinely assigned public facing internet IP addresses, we find a high IoT infection rate. In networks where carrier grade NAT is used, the infection rate is considerably reduced, because the vulnerable devices are not visible to network scanning.

With the introduction of 5G well underway, it is expected that not only the number of IoT devices will increase dramatically, but also the share of IoT devices accessible directly from the internet will increase as well. A separate section of this report analyzes the security challenges in the 5G environment and highlights the important role that Threat Intelligence can play in addressing security issues in multiple systems of the 5G architecture.

Android malware samples continue to grow in 2020

Figure 4 shows the increase in the mobile malware samples that were collected and analyzed in the Threat Intelligence Lab. There are now close to 27 million Android malware samples, which represents a 17.4% year-over-year increase.

Figure 4. Mobile malware samples in Threat Intelligence Lab's database



9 Threat Intelligence Report 2020

Nokia_Threat_Intelligence_Report_2020_Report_EN.pdf

35

How Do You Know If You Are Infected?

- Fans Spinning Wildly
- Programs start unexpectedly
- Your firewall yells at you
- Odd emails FROM you
- Freezes
- Your browser behaves funny
- Sudden slowness
- Change in behavior
- Odd sounds or beeps
- Random Popups
- Unwelcome images
- Disappearing files
- Random error messages

36

How Do You Know If You Are Infected?

- Fans Spinning Wildly
- Programs start unexpectedly
- Your firewall yells at you
- Odd emails FROM you
- Freezes
- Your browser behaves funny
- Sudden slowness
- Change in behavior
- Odd sounds or beeps
- Random Popups
- Unwelcome images
- Disappearing files
- Random error messages

You Don't

37

Your Browser Goes Rogue
If your browser has acquired new Toolbars/Extensions that you didn't install

People Receive Fraudulent Invitations/Emails From You
Threat actors set up fraudulent and copycat profiles on social media platforms and send invitations to the friends of the person with the real profile, or they gain access to the real profile probably through a phishing attack.

Passwords Mysteriously Change
If you cannot log in to an online service or platform, make sure the service is operational.

Software Materializes On Your Computer
If software appears on your computer and you have no idea where it came from, it might be enemy action.

The Cursor Flies Solo
A moving mouse pointer without your hand on the mouse may indicate hardware issues or be due to "drift" in the software drivers.

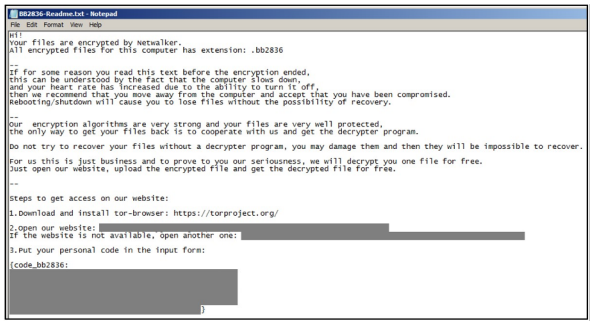
Your Shields Are Down And Won't Come Up
If your defensive software such as personal firewall, anti-virus, and anti-malware are turned off and refuse to come back into service, you've been infected with a virus or other malware.

Your Own Systems Tell You So
Any and all alerts from your intrusion detection system (IDS) or other monitoring software should be treated as genuine incidents until an investigation proves otherwise.

https://www.cloudsavvyit.com/7259/have-you-been-hacked-10-indicators-that-say-yes/

38

39



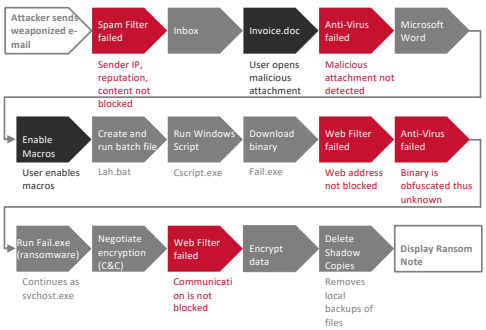
40

Your antivirus software is a seat belt – not a force field.

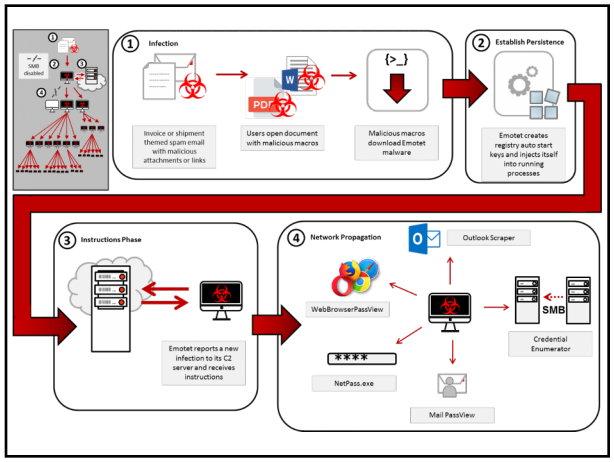
- *Alfred Huger*

41

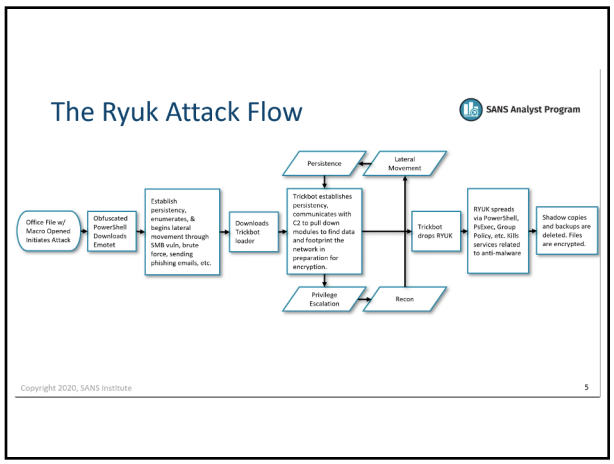
Infection Flow



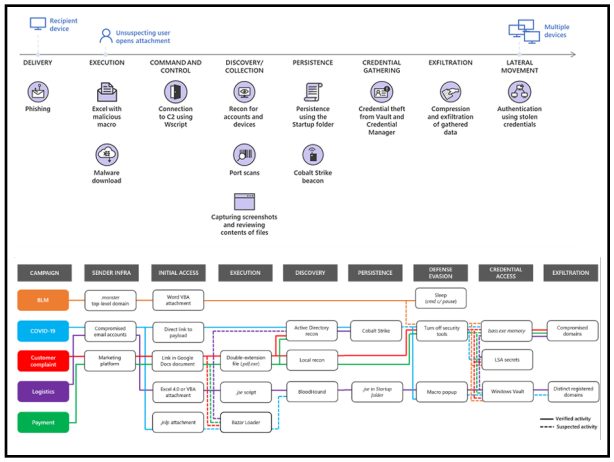
42


1 Infection
Invoice or shipment themed spam email with malicious attachments or links
Users open document with malicious macros
Malicious macros download Emotet malware
2 Establish Persistence
Emotet creates registry auto start keys and injects itself into running processes
3 Instructions Phase
Emotet reports a new infection to its C2 server and receives instructions
4 Network Propagation
Outlook Scraper
WebBrowserPassView
SMB
Credential Enumerator
NetPass.exe
Mail PassView

43


The Ryuk Attack Flow
SANS Analyst Program
Office File w/ Macro Opened initiates Attack
Obfuscated PowerShell Downloads Emotet
Establish persistency, enumerates, & begins lateral movement through SMB vuln, brute force, sending phishing emails, etc.
Downloads Trickbot loader
Persistence
Lateral Movement
Trickbot establishes persistency, communicates with C2 to pull down modules to find data and footprint the network in preparation for encryption.
Privilege Escalation
Recon
Trickbot drops RYUK
RYUK spreads via PowerShell, PsExec, Group Policy, etc. Kills services related to anti-malware
Shadow copies and backups are deleted. Files are encrypted.
Copyright 2020, SANS Institute
5

44


Recipient device
Unsuspecting user opens attachment
Multiple devices
DELIVERY
EXECUTION
COMMAND AND CONTROL
DISCOVERY/ COLLECTION
PERSISTENCE
CREDENTIAL GATHERING
EXFILTRATION
LATERAL MOVEMENT
Phishing
Excel with malicious macro
Malware download
Connection to C2 using Wscript
Recon for accounts and devices
Port scans
Capturing screenshots and reviewing contents of files
Persistence using the Startup folder
Cobalt Strike beacon
Credential theft from Vault and Credential Manager
Compression and exfiltration of gathered data
Authentication using stolen credentials
CAMPAIGN
SENDER INFRA
INITIAL ACCESS
EXECUTION
DISCOVERY
PERSISTENCE
DEFENSE EVASION
CREDENTIAL ACCESS
EXFILTRATION
BLM
COVID-19
Customer complaint
Logistics
Payment
Cobalt Strike
Bloodhound
Macro popup
Windows Vault
LSA secrets
Verified activity
Suspected activity

45

Phishing

IT experts...

The expert... **tries to make sense of the email**, and understand how it relates to other things in their life. As they do this, they notice discrepancies: little things that are "off" about the email. As the recipient notices more discrepancies, they feel a need for an alternative explanation for the email. At some point, some feature of the email — usually, the presence of a link requesting an action — triggers them to recognize that phishing is a possible alternative explanation.

At this point, **they become suspicious** (stage two) and investigate the email by looking for technical details that can conclusively identify the email as phishing.

Once they find such information, then they move to stage three and **deal with the email by deleting it or reporting it**.

https://dl.acm.org/doi/10.1145/3415231

46

Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender

Lee Hadlington, Jens Binder, and Natalia Stanulewicz

Published Online: 10 Jul 2020 https://doi.org/10.1089/cyber.2019.0703

Abstract

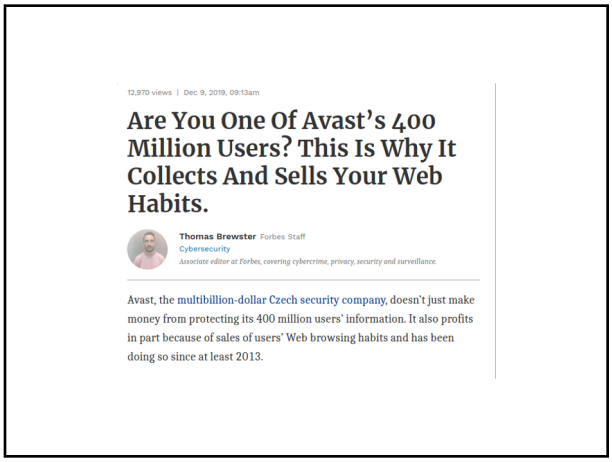
The role of human factors in employee information security awareness (ISA) has garnered increased attention, with many researchers highlighting a potential link between problematic technology use and poorer online safety and security. This study aimed to present additional evidence for this by exploring the relationship between of Fear of Missing Out (FoMO) and ISA in employees. A total of 718 participants completed an online questionnaire that included a measure of FoMO, ISA, as well as the Big Five personality inventory. Participants who reported higher levels of FoMO had lower overall ISA, as well as having poorer knowledge, a more negative attitude, and engaged in riskier behaviors in relation to ISA. **FoMO was also demonstrated to be the largest single negative predictor for ISA**, above that of age, gender, and the key personality traits tested. The potential reasons for the influence of FoMO over ISA are discussed, as well as the implications for organizational information security.

47

Locking Down Computers

- Keep Things Updated
  - The Operating System
  - All Applications (Browsers!)
- Application Allowlisting (whitelisting)
- Reboot to restore
- Secure Microsoft Office Macros
- Don't use Windows?
- What About Anti-virus Applications?

48



12,970 views | Dec 9, 2019, 09:13am

Are You One Of Avast's 400 Million Users? This Is Why It Collects And Sells Your Web Habits.

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Avast, the multibillion-dollar Czech security company, doesn't just make money from protecting its 400 million users' information. It also profits in part because of sales of users' Web browsing habits and has been doing so since at least 2013.

49

Securing The Other "Things" We use

50

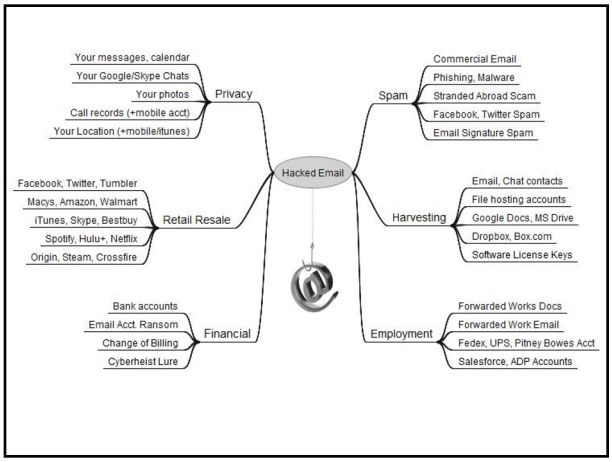
Which of your online accounts is most valuable?

- Email
- Bank
- Social Network
- Shopping
- Gaming
- Blogs

51

Own the Email, Own the Person

52

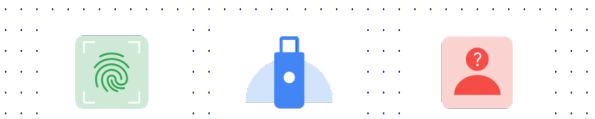


53

Second Factor Authentication

54

Types of additional information



Who you are | What you have | What you know

Google | Security and Privacy Group

55

Not all 2FA technologies are equal

	Secondary email	SMS verification	Device prompt	Security key
Boutique phishing	68%	96%	99%	100%
Spear-phishing	53-100%	76%	90%	100%

Evaluating Login Challenges as a Defense Against Account Takeover - WWW19

Google | Security and Privacy Group

56

The Consumer Authentication Strength Maturity Model (CASMM)

1	Token2FA	**Token-based 2FA** Examples: Yubikey, RSA Token. In addition to quality passwords in a manager, you authenticate using a physical token that only you have.	Vulnerable to: Token key system compromise, Live social engineering
2	App2FA	**App-based 2FA** Examples: Google Authenticator, Authy. In addition to quality passwords in a manager, you authenticate using an application that only you can access.	Vulnerable to: Live social engineering, Mobile device compromise
3	SMS2FA	**SMS-based 2FA** Examples: Any SMS-based auth. In addition to quality passwords in a manager, you authenticate using a text sent to your mobile device.	Vulnerable to: SIM-swapping, SMS-hijacking attacks
4	Password Manager	**Password Manager** Examples: 1Password, LastPass. In addition to having unique passwords, you also store them securely in an encrypted archive.	Vulnerable to: Account reset/takeover
5	Quality Passwords	**Quality Passwords** Examples: Aq!2-2vOe-T!oM. Your passwords are not just unique, but they're long, random, and they include special characters.	Vulnerable to: Password dumps / cracking
6	Unique Passwords	**Unique Passwords** Examples: DOBs, Tours, Schools. Your passwords are unique, but they're too short, simple, or contain personal information.	Vulnerable to: Live password guessing
7	Shared Passwords	**Shared Passwords** Examples: Gmail, Wells Fargo, Netflix. You use the same password in multiple places across the internet.	Vulnerable to: Credential stuffing

Daniel Miessler 2021

https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model-2/

57

Hacking

A Hacker Got All My Texts for $16

A gaping flaw in SMS lets hackers take over phone numbers in minutes by simply paying a company to reroute text messages.

By Joseph Cox

Looking down at my phone, there was no sign it had been hacked. I still had reception; the phone said I was still connected to the T-Mobile network. Nothing was unusual there. But the hacker had swiftly, stealthily, and largely effortlessly redirected my text messages to themselves. And all for just $16.

I hadn't been SIM swapped, where hackers trick or bribe telecom employees to port a target's phone number to their own SIM card. Instead, the hacker used a service by a company called Sakari, which helps businesses do SMS marketing and mass messaging, to reroute my messages to him. This overlooked attack vector shows not only how unregulated commercial SMS tools are but also how there are gaping holes in our telecommunications infrastructure, with a hacker sometimes just having to pinky swear they have the consent of the target.

https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

58

Phishing:

Fake email, telephone or text messages

59

Urgent Matter

JH John Herbert <smatteo@comcast.net>

Today, 12:44 PM

Blake Carver

Reply all

Action Items

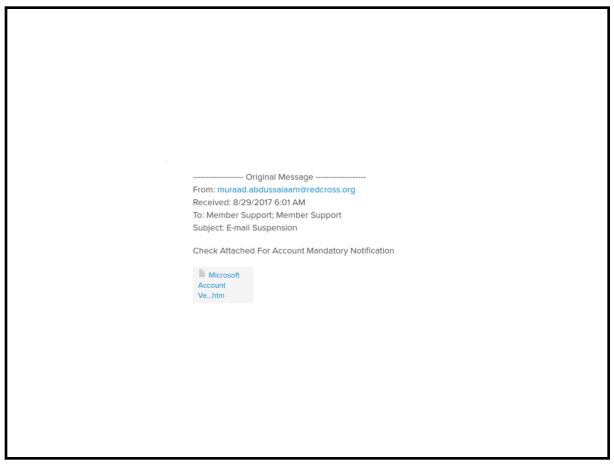
Hello Blake,

I need to know if you are available as i have something personal i would need you to assist with, I need you to please make a transfer to someone and for the amount of $5580 so by next week i will refund the money to you. Let me know if you can do this so as to send you the payee account information.

Regards,

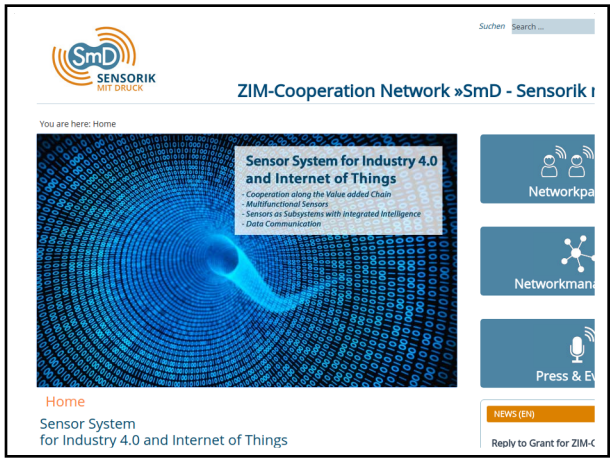
John Herbert

60


---------- Original Message ----------
From: muraad.abdussalaam@redcross.org
Received: 8/29/2017 6:01 AM
To: Member Support; Member Support
Subject: E-mail Suspension
Check Attached For Account Mandatory Notification
Microsoft Account Ve...htm

61

62


Suchen
Search ...
ZIM-Cooperation Network »SmD - Sensorik
You are here: Home
Sensor System for Industry 4.0 and Internet of Things
- Cooperation along the Value added Chain
- Multifunctional Sensors
- Sensors as Subsystems with integrated Intelligence
- Data Communication
Networkpa
Networkman
Press & E
Home
Sensor System
for Industry 4.0 and Internet of Things
NEWS (EN)
Reply to Grant for ZIM-C

63

Email

- Don't trust anything
- Don't leave yourself logged in
- 2 Factor Authentication
- Passwords
- Email is not a secure storage facility
- OpenPGP

64

Surfing The Web

65

The majority of encounters happen in the places that online users visit the most—and think are safe.

2013 Cisco Annual Security Report

66

Browsers

- Use Two & Keep Updated
- Know Your Settings
  - –Phishing & Malware Detection - Turned ON
  - –Software Security & Auto / Silent Patching - Turned **ON**
- A Few Recommended Extensions:
  - –Something to Limit JavaScript
  - –Something to Force HTTPS
  - –Something to stop trackers
  - –Something to Block Ads

67

Privacy Badger

uBlock Origin

uMatrix
???

HTTPS Everywhere

Disconnect

BROWSER

Ghostery

68

But The Internet Is Free Because Of Ads...

- Malicious content is 27 times more likely to be encountered via search engines than counterfeit software
- Online ads were 182 times more likely to deliver malware than an adult site

69

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS

SURPRISE —

Adblockers installed 300,000 times are malicious and should be removed now

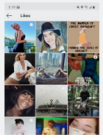
If you have Chromium versions of Nano Adblocker or Nano Defender, pay attention.

DAN GOODIN - 10/20/2020, 1:47 PM

113

Adblocking extensions with more than 300,000 active users have been surreptitiously uploading user browsing data and tampering with users' social media accounts thanks to malware its new owner introduced a few weeks ago, according to technical analyses and posts on Github.

Hugo Xu, developer of the Nano Adblocker and Nano Defender extensions, said 17 days ago that he no longer had the time to maintain the project and had sold the rights to the versions available in Google's Chrome Web Store. Xu told me that Nano Adblocker and Nano Defender, which often are installed together, have about 300,000 installations total.



Four days ago, Raymond Hill, maker of the uBlock Origin extension upon which Nano Adblocker is based, revealed that the new developers had rolled out updates that added malicious code.

70

Three million users installed 28 malicious Chrome or Edge extensions

Extensions could redirect users to ads, phishing sites, collect user data, or download malware on infected systems.

By Catalin Cimpanu for Zero Day | December 17, 2020 -- 02:30 GMT (18:30 PST) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Partial lists of organizations infected

71

How Amazon Assistant lets Amazon track your every move on the web

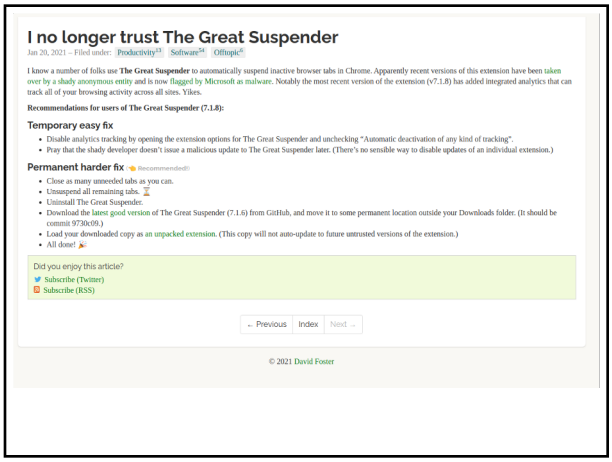
2021-03-08 amazon/privacy/security 16 mins 0 comments

I recently noticed that Amazon is promoting their Amazon Assistant extension quite aggressively. With success: while not all browsers vendors provide usable extension statistics, it would appear that this extension has beyond 10 million users across Firefox, Chrome, Opera and Edge. Reason enough to look into what this extension is doing and how.

Here I must say that the privacy expectations for shopping assistants aren't very high to start with. Still, I was astonished to discover that Amazon built the perfect machinery to let them track any Amazon Assistant user or all of them: what they view and for how long, what they search on the web, what accounts they are logged into and more. Amazon could also mess with the web experience at will and for example hijack competitors' web shops.

https://palant.info/2021/03/08/how-amazon-assistant-lets-amazon-track-your-every-move-on-the-web/

72



I no longer trust The Great Suspender

Jan 20, 2021 – Filed under: Productivity[13] Software[54] Offtopic[6]

I know a number of folks use **The Great Suspender** to automatically suspend inactive browser tabs in Chrome. Apparently recent versions of this extension have been taken over by a shady anonymous entity and is now flagged by Microsoft as malware. Notably the most recent version of the extension (v7.1.8) has added integrated analytics that can track all of your browsing activity across all sites. Yikes.

Recommendations for users of The Great Suspender (7.1.8):

Temporary easy fix

- Disable analytics tracking by opening the extension options for The Great Suspender and unchecking "Automatic deactivation of any kind of tracking".
- Pray that the shady developer doesn't issue a malicious update to The Great Suspender later. (There's no sensible way to disable updates of an individual extension.)

Permanent harder fix Recommended!

- Close as many unneeded tabs as you can.
- Unsuspend all remaining tabs.
- Uninstall The Great Suspender.
- Download the latest good version of The Great Suspender (7.1.6) from GitHub, and move it to some permanent location outside your Downloads folder. (It should be commit 9730c09.)
- Load your downloaded copy as an unpacked extension. (This copy will not auto-update to future untrusted versions of the extension.)
- All done!

Did you enjoy this article?
Subscribe (Twitter)
Subscribe (RSS)

← Previous | Index | Next →

© 2021 David Foster

73

KrebsonSecurity
In-depth security news and investigation

01 Is Your Browser Extension a Botnet Backdoor?

MAR 21

A company that rents out access to more than 10 million Web browsers so that clients can hide their true Internet addresses has built its network by paying browser extension makers to quietly include its code in their creations. This story examines the lopsided economics of extension development, and why installing an extension can be such a risky proposition.

Singapore-based **Infatica[.]io** is part of a growing industry of shadowy firms trying to woo developers who maintain popular browser extensions — desktop and mobile device software add-ons available for download from **Apple**, **Google**, **Microsoft** and **Mozilla** designed to add functionality or customization to one's browsing experience.

Some of these extensions have garnered hundreds of thousands or even millions of users. But here's the rub: As an extension's user base grows, maintaining them with software updates and responding to user support requests tends to take up an inordinate amount of the author's time. Yet extension authors have few options for earning financial compensation for their work.

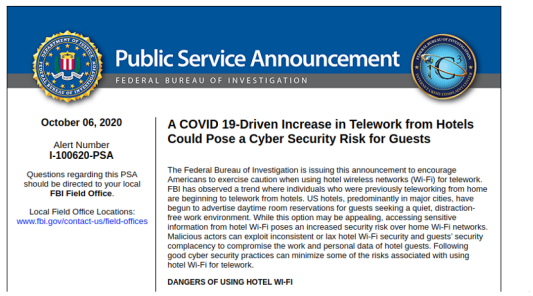
https://krebsonsecurity.com/2021/03/is-your-browser-extension-a-botnet-backdoor/

74

Never Trust Public Wi-Fi

Use A PAID VPN

75



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 06, 2020

Alert Number
I-100620-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

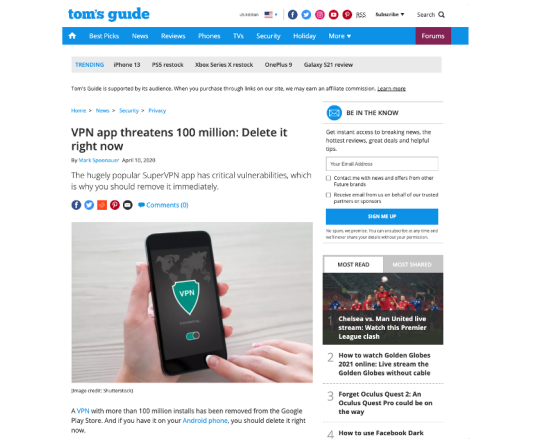
Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

A COVID 19-Driven Increase in Telework from Hotels Could Pose a Cyber Security Risk for Guests

The Federal Bureau of Investigation is issuing this announcement to encourage Americans to exercise caution when using hotel wireless networks (Wi-Fi) for telework. FBI has observed a trend where individuals who were previously teleworking from home are beginning to telework from hotels. US hotels, predominantly in major cities, have begun to advertise daytime room reservations for guests seeking a quiet, distraction-free work environment. While this option may be appealing, accessing sensitive information from hotel Wi-Fi poses an increased security risk over home Wi-Fi networks. Malicious actors can exploit inconsistent or lax hotel Wi-Fi security and guests' security complacency to compromise the work and personal data of hotel guests. Following good cyber security practices can minimize some of the risks associated with using hotel Wi-Fi for telework.

DANGERS OF USING HOTEL WI-FI

76



tom's guide

Best Picks | News | Reviews | Phones | TVs | Security | Holiday | More | Forums

TRENDING iPhone 13 | PS5 restock | Xbox Series X restock | OnePlus 9 | Galaxy S21 review

Tom's Guide is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Learn more

Home > News > Security > Privacy

VPN app threatens 100 million: Delete it right now

By Mark Spoonauer April 10, 2020

The hugely popular SuperVPN app has critical vulnerabilities, which is why you should remove it immediately.

Comments (0)

(Image credit: Shutterstock)

A VPN with more than 100 million installs has been removed from the Google Play Store. And if you have it on your Android phone, you should delete it right now.

BE IN THE KNOW

Get instant access to breaking news, the hottest reviews, great deals and helpful tips.

Your Email Address

Contact me with news and offers from other Future brands

Receive email from us on behalf of our trusted partners or sponsors

SIGN ME UP

No spam, we promise. You can unsubscribe at any time and we'll never share your data without your permission.

MOST READ | MOST SHARED

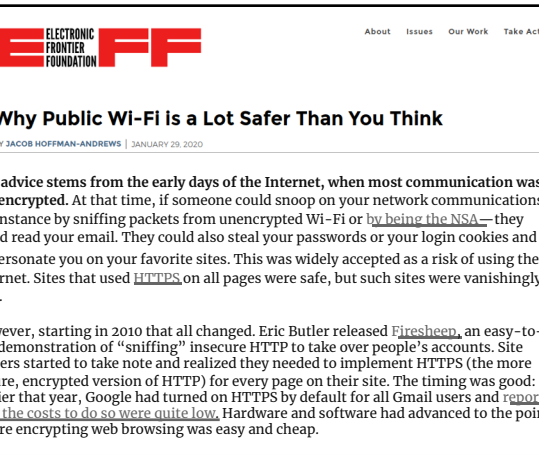
1 Chelsea vs. Man United live stream: Watch this Premier League clash

2 How to watch Golden Globes 2021 online: Live stream the Golden Globes without cable

3 Forget Oculus Quest 2: An Oculus Quest Pro could be on the way

4 How to use Facebook Dark

77



ELECTRONIC FRONTIER FOUNDATION

About | Issues | Our Work | Take Action

Why Public Wi-Fi is a Lot Safer Than You Think

BY JACOB HOFFMAN-ANDREWS | JANUARY 29, 2020

The advice stems from the early days of the Internet, when most communication was not encrypted. At that time, if someone could snoop on your network communications—for instance by sniffing packets from unencrypted Wi-Fi or by being the NSA—they could read your email. They could also steal your passwords or your login cookies and impersonate you on your favorite sites. This was widely accepted as a risk of using the Internet. Sites that used HTTPS on all pages were safe, but such sites were vanishingly rare.

However, starting in 2010 that all changed. Eric Butler released Firesheep, an easy-to-use demonstration of "sniffing" insecure HTTP to take over people's accounts. Site owners started to take note and realized they needed to implement HTTPS (the more secure, encrypted version of HTTP) for every page on their site. The timing was good: earlier that year, Google had turned on HTTPS by default for all Gmail users and reported that the costs to do so were quite low. Hardware and software had advanced to the point where encrypting web browsing was easy and cheap.

78

Social Media

- Understand and adjust your privacy settings
- Be skeptical of everything –especially ANYONE asking you for money

79

Free Services Are Expensive

"...if you're not the customer you're the product being sold"

metafilter.com/95152

80

Mobile Devices - Threats

- Trojans, Viruses & Malware
- Lost and/or Stolen
- Opaque Apps Permissions
- Access To Everything
- Open Wi-Fi Networks and Public Hotspots
- Data leakage
- Insecure Wi-Fi
- Network spoofing
- Phishing and social engineering attacks
- Spyware
- Poor cyber hygiene, including weak passwords and improper or no use of multifactor authentication (MFA)
- Poor technical controls, such as improper session handling, out-of-date devices and operating systems, and cryptographic controls

81

Mobile / Portable / Cellular

Solid Operating Systems
Encrypted
Super Secure Hardware (secure enclave)
End to end secure apps available
Biometrics

82

But...

Endless Apps means endless points of insecurity

OS design can hide really bad practices

lack of TLS, client app no longer validates certs, bad coding, basic security stuff

You don't see it in the UI

83

The privacy is even worse...

More apps collecting more stuff storing it in more places and sharing widely

84

Current attacks are generally tough & against High Value Targets

High value most often means rich financial gains for the threat actors.

They require significant financial backing, top-tier technical skills, a lot of man-power, and operational guidance and control.

Riskware is the name used for free apps that offer to do something entertaining or useful—and actually deliver on that promise—but secretly siphon off information and send it back to the app publishers to be sold to advertisers or criminals.

- Smishing Attacks
- Loss / Swiper got swiped
- SIM Swapping
- Public Wi-Fi and Network Spoofing

https://www.cloudsavvyit.com/8514/why-cyber-criminals-love-cellphones/

85

Set up a mobile carrier PIN

SIM hijacking is a process where a hacker socially engineers or bribes a mobile carrier to transfer your phone number to a SIM card they own.

If you use text messages as a two-factor authentication method, this gives hackers the ability to bypass 2FA and in most cases the ability to reset your passwords completely.

86

Mobile Devices

1. Encrypt it
2. Password it
3. Backup it
4. Case it
5. Know those settings
6. Watch your Wifi
7. It is not forever

87

How do you know if you have malware on your phone?

- You see ads all the time.
- You install an app and it disappears immediately.
- Your battery drains much faster than usual.
- You see apps that you don't recognize.
- Data usage through the roof.
- Random charges on your phone bill.
- Slow.
- Your friends get weird messages/emails from you

88

Carry A Safe
Not A Suitcase

89