CYBER SECURITY BASICS

especially prepared for:

https://endtransplantabuse.org/
WHY?

Ask a fortune teller..

It is always in the news..

Because your devices know ALOT about you....

Security? That is just my password right?
Chinese Hackers Used a New Rootkit to Spy on Targeted Windows 10 Users

October 01, 2021  Ravi Lakshmanan

A formerly unknown Chinese-speaking threat actor has been linked to a long-standing evasive operation aimed at South East Asian targets as far back as July 2020 to deploy a kernel-mode rootkit on compromised Windows systems.

NSO Groups Pegasus malware...
WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Ted Talk...
What your smart devices know (and share) about you..

https://www.youtube.com/watch?v=POHYyP4EbzE

Are your account details already compromised?

https://haveibeenpwned.com
PASSWORD STRENGTH CHECKER?

How Secure is Your Password?

- https://howsecureismypassword.net
- https://www.passwordmonster.com
SO YOU WANT TO PROTECT YOUR EMAIL...
HOW BAD GUYS CAN ‘HACK’ YOU....

WHY DON'T YOU JUST TELL ME?

https://www.youtube.com/watch?v=RfAdux3XidM

What's your password?!
PASSWORDS - DO’S AND DON'TS

Do's
- use a password manager
- use unique passwords
- keep passwords to yourself!
- use MFA (covered later)

Don'ts
- Don't use the same password everywhere!
- Don't save passwords in your browser
- Don't save passwords in a file on your computer
PASSWORD MANAGERS TO THE RESCUE

ACTION

Install and use a password manager!
Local Install
  • KeePassXC - https://keepassxc.org (recommended! Win/macOS/Linux)

Cloud based
  • bitwarden
  • Lastpass
  • 1password

ACTION - SETUP MFA

A security measure that requires two or more proofs of identity to grant you access

Multi-factor authentication (MFA) typically requires a combination of something the user knows (pin, secret question), physically possesses (card, token) or inherently possesses (finger print, retina).

Significantly more powerful security

The multiple layers make it much harder for criminals to attack your business. Criminals might manage to steal one proof of identity e.g. PIN, but they still need to obtain and use the other proofs of identity. Two-factor authentication (2FA) is the most common type of MFA.

- Turning on Two-Factor Authentication - Apple ID
- Turning on Two-Factor Authentication - Facebook
- Turning on Two-Factor Authentication - Facebook Messenger
- Turning on Two-Factor Authentication - Gmail
Is your email account safe?
HAVE YOU NOTICED..

- people are telling you they are receiving emails from you that you didn't send?

ASK YOUR TECH PERSON TO HELP..

- check your 'sent' items
- suspicious access attempts?
- suspicious 'forwarding' rules
EMAIL PROVIDERS - THAT CARE ABOUT PRIVACY!

About Tutanota
Tutanota is the world's first end-to-end encrypted mail service that encrypts the entire mailbox. With its unique open source technology Tutanota fights for privacy and freedom of speech online. Started as a secure email service in 2011, Tutanota now offers an encrypted address book, an encrypted calendar and the encrypted contact form Secure Connect.

In addition, Tutanota’s affordable business version enables companies and organisations of all sizes to easily secure their email communication.

https://tutanota.com

We're building an internet that protects privacy, starting with email.

We are scientists, engineers, and developers drawn together by a shared vision of protecting civil liberties online. This is why we created ProtonMail, an easy to use secure email service with built-in end-to-end encryption and state of the art security features.

Our goal is to build an internet that respects privacy and is secure against cyberattacks.

https://protonmail.com
**ACTIONS**

Netcraft browser extension!
https://www.netcraft.com/apps/browser/

**MORE...**

DNS services. eg.,
https://www.opendns.com/home-internet-security/
OR
https://cleanbrowsing.org/filters/
SO YOU WANT TO PROTECT YOUR IDENTITY?
So you want to buy a coffee?

Review your Facebook settings!

https://reclaimthenet.org/facebook-privacy-settings/

https://www.youtube.com/watch?v=yrjT8m0hcKU
WHAT IS VPN AND SOME PROVIDERS

Your real IP can reveal your location eg., geoip demo

https://www.whatismyip.com

use a VPN to 'hide' your location and 'pretend' to be somewhere else
WHICH VPN SHOULD I USE?

ANY VPN IS STILL BETTER THAN NONE!

NORD VPN
https://nordvpn.com

SURFSHARK
https://surfshark.com

why nord and surfshark?
https://restoreprivacy.com/vpn/comparison/nordvpn-vs-surfshark/
https://restoreprivacy.com/vpn/comparison/expressvpn-vs-surfshark/
**SECURE MESSAGING**

- signal - [https://signal.org](https://signal.org) (recommended by Snowden!)
- telegram? (review and decide yourself!)

For additional security (to not disclose your phone number): register accounts with a different SIM card!
PROTECT YOUR DATA...
Do you have any of these hobbies?
- [ ] Are you a cruise enthusiast?
- [ ] Are you a fitness and exercise buff?
- [ ] Are you interested in foreign travel?

Do you own an aircraft?
- [ ] Yes
- [ ] No

Do you own a boat?
- [ ] Yes
- [ ] No

Do you exercise or participate in other activities to lose weight?
- [ ] Yes
- [ ] No

$0.6714
Current value of my data
**PII Confidentiality Impact Levels**

**LOW**
- Full Name
- Date of Birth
- Place of Birth
- Mother's Maiden Name
- Home Address
- Home Phone Number

**MEDIUM**
- Full name + any low risk information EXCEPT:
  - Full Name + EDI PI (DoD ID Number on Back of CAC) = (Low)
  - Full Name + Office Information = (Low)
  - Full Name + Rank = (Low)
  - Full Name + Award = (Low)
- Any information that could cause direct harm on its own

**HIGH**
- Full Social Security Number (SSN)
- Last 4 digits of SSN
- Full Name + Financial Data
- Full Name + Medical Data
- Full Name + Biometric Data
- Full Name + Driver License Number
Your weakest link: All those online accounts you’ve forgotten about

Actually, that number is more likely in the hundreds. According to Dashlane, the average American had 150 online accounts in 2017, and they predicted that this number could reach 300 by 2022. It’s 2020 now, and each of us probably has more than 200 accounts—because of the ones we don’t even remember. Most of the online services and apps you use require you to create a username and some form of authentication.

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

MySpace: In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the “Real Deal” dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

Compromised data: Email addresses, Passwords, Usernames

Oxfam: In January 2021, Oxfam Australia was the victim of a data breach which exposed 1.8M unique email addresses of supporters of the charity. The data was put up for sale on a popular hacking forum and also included names, phone numbers, addresses, genders and dates of birth. A small number of people also had partial credit card data exposed (the first 6 and last 3 digits of the card, plus card type and expiry) and in some cases the bank name, account number and BSB were also exposed. The data was subsequently made freely available on the hacking forum later the following month.

Compromised data: Bank account numbers, Dates of birth, Email addresses, Genders, Names, Partial credit card data, Payment histories, Phone numbers, Physical addresses

tumblr: In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

Compromised data: Email addresses, Passwords
LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords hacked in 2012, the data remained out of sight until being offered for sale on Dark Web forums last year. The passwords in the breach were stored as SHA1 hashes with some of them successfully cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

MySpace: In approximately 2008, MySpace suffered a data breach that exposed the personal information of millions of users. In May 2016 the data was offered up for sale on the "Real Deal" data breach forum, which included email addresses, usernames and SHA1 hashes of the first 10 characters of the passwords. The passwords were converted to lowercase and stored without a salt. The exact breach date is unknown and the data suggests it was 6 years before being made public.

Compromised data: Email addresses, Passwords, Usernames

Oxfam: In January 2021, Oxfam Australia was the victim of a data breach which exposed the email addresses of supporters of the charity. The data was put up for sale on forums and included names, phone numbers, addresses, genders and dates of birth. The data was later put up for sale on a dark market website and passwords were sold as SHA1 hashes.

Compromised data: Email addresses, Passwords

Box
EASY
NO INFO AVAILABLE

eBay
EASY
SHOW INFO...

Facebook
MEDIUM
SHOW INFO...

Google
EASY
NO INFO AVAILABLE

Groupon
HARD
SHOW INFO...

GoDaddy
IMPOSSIBLE
SHOW INFO...

Instagram
EASY
NO INFO AVAILABLE

LinkedIn
MEDIUM
SHOW INFO...

Match
MEDIUM
SHOW INFO...

tumblr
In early 2013, Tumblr suffered a data breach which resulted in the exposure of approximately 70 million accounts. The database was put up for sale on Dark Web forums and passwords were sold as SHA1 hashes.

Compromised data: Email addresses, Passwords

Have I Been Pwned? Check if your email or phone is in a data breach.
How to Find Those Old Online Accounts You Don’t Remember

1. Create a list of all your online accounts.
2. Use a password manager.
3. Update the passwords for your existing accounts.
4. Sift through your old emails.
5. Check data leakage tracking sites.
6. Employ username checking sites.
7. Look for your data on search engines.
8. Repeat your security spring cleaning once a year.

for this guide and more visit accountkiller.com

AccountKiller was featured in leading news and technology resources, including

© 2011-2020 ACCOUNTKILLER.COM | Terms of Service | Privacy Policy
BUY OLD LINKEDIN ACCOUNTS

$30.00 – $12,600.00

- Old LinkedIn Accounts
- Manual Create Accounts
- Male Or Female Accounts
- 100% Satisfaction Guaranteed.
- 48 Hours Free Replacement Warranty
- No specific country, it will be worldwide
- High-quality service
- Unique IP Created
- Instant Start on your Purchase
- 24/7 Premium Customer Support

- Delivery in File Format Excel Sheet/Notepad
- I will complete your order maximum time in 48/72 Hours

Connect for details my Skype ID: Bestsocialwork

SELECT PACKAGE ➤ 5+ Accounts 250+ Connection (1 yer) Old ($150)

$150.00
The more of your data I gather, the more I understand what it means to be human.

Mark Zuckerberg..... the Count Dracula of Data Harvesting
Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too.

A Palestinian hacker who said he had breached Mark Zuckerberg’s Facebook profile showed the page in 2013. Hazem Bader/Agence France-Presse — Getty Images
Olixar for Amazon Echo Show Camera Cover - Privacy Slide - Webcam Cover - Compatible With Laptops, Tablets & Smartphones - Anti Hack Security - 3 Pack

Brand: Olixar

32 ratings

About this item

- KEEP YOUR FAMILY SAFE Avoid being cyber hacked and being spied on by keeping your Amazon Echo Show's camera covered
- COVER MULTIPLE DEVICES 3 pack - universally compatible design makes the covers universally compatible with laptops, tablets and smartphones
- STYLISH &MINIMALIST DESIGN 1mm thick - small, ultra-thin and discreet design allows the cover to be barely noticeable
- STICK ONCE, KEEP FOREVER Stainless steel sliding construction with a 3M adhesive surface ensures the cover remains attached
- 2 YEAR WARRANTY 2 year Olixar manufacturer warranty
All your friends are posting aging selfies with FaceApp - a Russian app that's raising privacy concerns

BY CHRISTOPHER BRITO
July 17, 2019 / 4:51 PM / CBS News
How people think they get hacked

How they really get hacked

- If you had to marry your spouse where you met them, where would your wedding have been?
- Your porn name is your middle name and the first car you had.
- The car you passed your drivers test in was a ____
- Asking where you’d get married again is like asking where you met.
- A ‘porn name’ that exposes your middle name AND a street you grew up on are TWO pieces of info that people need.

Find Your Rapper Name!
Pick the month you were born:
- Jan - Hood
- Mar - Squagly
- May - Squagly
- July - Tuff
- Sept - Shiny
- Oct - Loy

It's Throwback Thursday!
What was the name of your childhood pet?
Cambridge Analytica Ltd (CA) was a British political consulting firm that combined misappropriation of digital assets, data mining, data brokerage and data analysis with strategic communication during the electoral processes.
How can I tell if my info was shared with Cambridge Analytica?

Recently, we shared information about the potential misuse of your data with academic and research websites. We also shared plans for how we're taking action to prevent it in the future.

Check below to see if your information has been shared with the app “This Is Your Digital Life.”

Was my information shared?

Based on our investigation, you don't appear to have logged into "This Is Your Digital Life" with Facebook before we removed it from our platform in 2015.

However, a friend of yours did log in.

As a result, the following information was likely shared with "This Is Your Digital Life":

- Your public profile, Page likes, date of birth and current city
Restrict Google Activity by setting Web & app activity, location, and Youtube history to "Off".
Permission Model

Android implements a permission model for individual apps

- Applications must declare which permissions (in the manifest file) they require
- When the application is installed, Android will present the permission list to the user so that he can view the list and allow installation or not
Technique: Smudge attack

- Infer the lock pattern from the oil smudge left on the display’s surface
  - First responders must minimize contact with the screen
App Cleaner & Uninstaller

- Manage installed applications
- Remove broken service files
- Manage system extensions
- Disable unneeded startup programs
- Clean up and uninstall applications
China spent years collecting Americans' personal information. The U.S. just called it out.

Beginning around 2014, a host of American organizations were hacked, with the government and private cybersecurity firms naming China as the culprit.

China has enough stolen US data to create 'dossiers' on every American, Senate panel is told
WHY DO I STILL NEED ANTI-VIRUS?

(YES! ransomware is big business!)

How it works:
1) obtain sample
2) create 'vaccine'
3) distribute 'vaccine'

CHALLENGE:
infinite mutations in an instant!
WHY DO I STILL NEED ANTI-VIRUS?

is AV 'broken'? can AV keep up?
Stuart McClure, a former McAfee executive, is 'infamous' for not running his own companies product!

Q: You stuck around after McAfee bought Foundstone but you later became famous — or infamous — for telling the world that you didn’t use anti-virus software? That takes brass.

It does. But I have an anaphylactic response to untruths. I was asked to do a talk at the Rochester Institute of Technology. At the end of my presentation, a student asked me to show him my system tray, he said he wanted to know what I ran on my computer to protect myself. I looked at the front row and there’s the head of worldwide sales for McAfee sitting there. I’m like, you’ve got to be kidding me. Anyway, I said, “Look I don’t need to show you my system tray, I will tell you that I don’t use any security products and I haven’t since 1995.” This was in 2004.

https://medium.com/@DFJvc/stuart-mcclure-cylance-464f71285aaf
WHICH AV SHOULD I USE?

Cylance Smart AV
https://shop.cylance.com/us

Webroot AV

Both are available for PC, Mac and mobile!
WHY CYLANE SMART AV?

HOW it works

- Machine Learning & AI trained with millions of computer viruses to distill the "DNA" of a computer virus
- looks at numerous 'features' to 'score' a file as 'good' or 'bad'
- PREVENTS the virus from ever running on the computer!
WHY WEBROOT?

HOW it works

• known good file - allow
• known bad file - block and quarantine
• unknown file - run and 'record' every action
  • if suspicious activity - 'undo' every single action
• check against 'cloud' when required
• Webroot Brightcloud threat intelligence
WHY WEBROOT? BRIGHTCLOUD THREAT INTELLIGENCE

Webroot coverage includes:

- 27+ Billion URLs
- 600+ Million Domains
- 4+ Billion IP Addresses
- 15+ Billion File Behavior Records
- 62+ Million Mobile Apps
- 57+ Million Connected Sensors
**KEEP YOUR SOFTWARE UPDATED!**

- keep Windows/macOS updated
- keep applications updated

PatchMyPC home updater for Windows!
https://patchmypc.com/home-updater

How to install PatchMyPc (free!)
https://www.youtube.com/watch?v=y5WWiWbO6v0
AES encryption!

Advanced Encryption Standard

From Wikipedia, the free encyclopedia

The Advanced Encryption Standard (AES), also known by its original name Rijndael (Dutch pronunciation: [ˈrɛindaːl]),[3] is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.[4]

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
7-ZIP (WINDOWS)

https://www.7-zip.org
ENCRYPTING WORD DOCUMENTS

https://en.wikipedia.org/wiki/Microsoft_Office_password_protection

Office 2013 (Access, Excel, OneNote, PowerPoint, Project, and Word) uses 128-bit AES, again with hash algorithm SHA-1 by default.1

Office 2016 (Access, Excel, OneNote, PowerPoint, Project, and Word) uses 256-bit AES, the SHA-1 hash algorithm, and CBC (Cipher Block Chaining) by default.1
CUTE PDF WRITER TO PROTECT PDFS (WINDOWS)

https://www.cutepdf.com/Products/CutePDF/writer.asp
TIME FOR ACTION..
TOP ACTIONS

If you only did 3 things..
- MFA
- Anti-virus
- social accounts!!
- (plus) backups!
ACTIONS TO PROTECT YOUR ACCOUNTS AND EMAIL LOGINS

- setup MFA

- install and use a password manager
  https://keepassxc.org

- install the Netcraft web filter!
  https://www.netcraft.com/apps/browser
ACTIONS TO PROTECT YOUR IDENTITY ONLINE

• review your social media privacy settings
  https://reclaimthenet.org/facebook-privacy-settings/

• use a VPN to hide your true location
  https://nordvpn.com (Windows/macOS/mobile)
  https://surfshark.com (Windows/macOS/mobile)
SIMPLE ACTIONS TO PROTECT YOUR DATA

- Install antivirus
  https://shop.cylance.com

- Update your software
  https://patchmypc.com/home-updater

- backup your data!
- learn to encrypt your data!
  - 7-zip passwords with AES encryption
  - password protection on MS docs and pdf's
VIDEOS

Amazing mind reader reveals his 'gift'
https://www.youtube.com/watch?v=F7pYHN9iC9I

How Private is your personal information?
https://www.youtube.com/watch?v=yrjT8m0hcKU

What's your password?
https://www.youtube.com/watch?v=yrjT8m0hcKU
POSTERS AND INFOGRAPHICS

Passwords and passphrases
https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Posters and infographics for Ransomeware, Phishing, Passwords, etc..
https://www.ncsc.gov.uk/information/infographics-ncsc