30-day Security Challenge Syllabus

The 30-day security challenge was developed by Shannon Morse of Hak5 acclaim. It's a comprehensive overview of basic cybersecurity hygiene for the average person.

Prerequisites: Watch this video (and start taking the challenge!)

Instructor:

Charles Blas (charles@hackerlab.org)

Office Hours:

TBD

Audience

This course is appropriate for anyone that interacts with the Internet. The primary audience is over 17 years old, but teenagers can attend with parent/guardian consent. There is no upper age limit.

People with 1-3 years of experience in big corporations may be familiar with some of the content because it is similar to most corporate cybersecurity awareness classes.

People with 1-2 years of experience in a cybersecurity/technical field may find the material too remedial or simplistic. In that case, you might get more from the course if you volunteer to teach or TA instead. We will conduct train-the-trainer sessions before the next 30-day challenge and those sessions will not be publicised. So, sign up to volunteer here.

Course Description

The weekly classes will serve as a support group for those who embark on the security challenge. The full security challenge is outlined here.

This course will introduce basic security concepts that encompass almost all activities of online life. The Monday sessions will serve as a recap of activities of the previous week and a preview of the week ahead. Most of the time will be spent in discussion and students will be expected to interact. To get the most value out of this course, students are encouraged to go through the actual security challenge, write down your questions, and bring them to class. Classes will not conclude until all questions have been satisfactorily answered.

Major Instructional Areas

Over the course of the 30-day challenge, we will explore:

- General best practices around device (computer, phone, wifi router, IoT, etc...) security
- Basics of encryption and authentication
- Wireless protocols (e.g. Bluetooth, wifi, NFC)
- Anti-virus, anti-malware software

- Browser security
- Privacy controls
- Social accounts and maintenance
- Smartphone apps
- Computer backups
- Cloud services
- Two-factor authentication (2FA) or multi-factor authentication (MFA)
- Virtual Private Network (VPN)
- Passwords and password managers
- Single sign-on technologies
- Spear-Phishing
- Social engineering
- Credit card security
- Public databases

Course Objectives

The entire course is meant to be an introduction to cybersecurity best practices. After successful completion of the full course, the student will have the opportunity to:

- Establish goals for cybersecurity hygiene and measure their progress and completion.
- Understand the risk associated with stale, abandoned accounts
    - Discover effective strategies for handling old accounts
- Understand how to securely ‘factory wipe’ devices and why you should do that before selling any of you return or resell your technology
- Understand the basic wireless encryption protocols: WEP, WPA, WPA2
- Recognize when it’s time to upgrade your wifi router, and what to look for in an upgrade
- See the benefits of using a guest network to manage Internet of Things (IoT) devices
- Setup encryption, lock screens, and theft controls on phones
- Understand the risk of Bluetooth, NFC and how to control the risk
- Explore antivirus and antimalware technology and choose the best solution for your needs
- Understand basic browser security and privacy controls for the major browsers (e.g. Chrome, Firefox, Brave, etc…)
- Basic security hygiene related to email and Internet browsing (e.g. how do you know if a link is safe to click)
- Evaluating security of smartphone apps
- Realize the benefit of backups by looking at it from a cost/benefit perspective
- Gain experience with password managers and understand the trade-offs between the major providers (e.g. LastPass, Dashlane, etc…)
- Understand the basics of multi-factor authentication: what is the user experience, how secure is it?
- Explore different VPN technologies (e.g. OpenVPN, Wireguard) and contrast the differences between the technologies and the providers
- Understand the basics of friend lists and how your friends affect your security and privacy
- Understand basic smartphone application permissions and evaluate their appropriateness
- Develop best practices to securely authenticate to websites
- Explore security and privacy options in common online mail platforms
- Have hands on experience playing with encryption
- Understand how social engineering attacks work, and how to cope

- See the tools and techniques used by credit card fraudsters
- Develop a strategy to securely opt out of public databases
- See how a Faraday Bag works

Teaching Strategies

The weekly classes will serve as a support group for those who embark on the security challenge. The full security challenge is outlined here.

Shannon has recorded videos and annotated with text, so you can follow along at your own pace. If you're actually doing the work, it is expected that you will pause the video many times. Some daily challenges are short and quick and can be accomplished in 15 minutes. Others require doing a lot of homework and may take days or weeks to fully complete (e.g. transitioning to using a password manager).

In each class session, we will summarize the activities of the previous and give an overview of activities for the following week; we will assume that everyone starts the challenge on April 26 or so. Ideally, you would be taking the challenge in real time and writing down your questions to bring to class.

In addition to the weekly summary classes, there will be a discord channel where you can ask questions anytime.

Also, there will be Saturday sessions where we will walk through the process of: securing your wifi, setting up a VPN, and opting out of public databases. Students are encouraged to prepare ahead of time and follow along in real time.

Course Resources

Online support forum (discord): https://discord.gg/DVs8FG7Aey

Walkthroughs for Hacker Lab sessions:

- Securing your home wifi network:
  https://hackerlab.org/files/30-daySecurityChallenge-Walkthrough-Wifi.pdf

- Anything you ever wanted to know about VPNs:
  https://hackerlab.org/files/30-daySecurityChallenge-Walkthrough-VPNs.pdf

- Properly opting-out of public databases
  https://hackerlab.org/files/30-daySecurityChallenge-Walkthrough-OptingOut.pdf

Links from the actual 30-day Security Challenge

- Day 2: Delete Old Accounts & Factory Wipe Old Devices
  - https://backgroundchecks.org/justdeleteme/
  - https://plaintextoffenders.com/
- Day 3: Protect Your Home Network and Set Up a Guest Network
  - https://www.nytimes.com/wirecutter/reviews/best-wi-fi-router/
  - https://www.nytimes.com/wirecutter/reviews/best-cable-modem/
  - https://www.grc.com/shieldsup
- Day 5: Setting Up Encryption, Lock Screens, FindMyDevice & Auto Updating

  - Setting up your lock screen
    - https://support.google.com/nexus/answer/2819522?hl=en
    - https://www.imore.com/lock-screen
  - Smartphones are easy to encrypt and lock down!
    - https://ssd.eff.org/en/module/how-encrypt-your-iphone
    - http://www.androidauthority.com/how-to-encrypt-android-device-326700/
    - https://www.lifewire.com/encrypt-the-data-on-your-android-phone-or-iphone-2377707
  - Using Find My Device
    - https://www.google.com/android/find
    - https://support.apple.com/explore/find-my-iphone-ipad-mac-watch
    - https://support.google.com/android/answer/6160491?hl=en
  - Update your phone
    - https://support.google.com/nexus/answer/4457705?hl=en
    - https://support.apple.com/en-us/HT204204
  - Encrypt your hard drive
    - https://support.apple.com/kb/PH25553?locale=en_US
      - (updated: https://support.apple.com/en-us/HT204837)
    - https://www.howtogeek.com/234826/how-to-enable-full-disk-encryption-on-windows-10/
    - https://support.microsoft.com/en-us/help/4028713/windows-turn-on-device-encryption
    - https://www.veracrypt.fr/en/Home.html
  - Find your Computer
    - https://support.microsoft.com/en-us/help/11579/microsoft-account-find-lost-phone-device
    - https://support.apple.com/explore/find-my-iphone-ipad-mac-watch
    - https://account.microsoft.com/devices
  - Update your Computer
    - https://support.apple.com/en-us/HT201541
    - https://support.microsoft.com/en-us/help/12373/windows-update-faq
- Day 7: AntiVirus and AntiMalware Software Apps
  - https://www.avast.com/free-antivirus-download
  - https://www.malwarebytes.com/premium/
  - https://www.microsoft.com/en-us/windows/windows-defender
  - https://www.microsoft.com/en-us/wdsi/products/scanner
  - https://www.bitdefender.com/solutions/antivirus-for-mac.html
- Day 8: Time for a Better Browser!
  - https://support.apple.com/en-us/HT201607
  - https://support.microsoft.com/en-us/help/4028606/windows-change-your-default-browser-in-windows-10
  - https://allaboutdnt.com/
  - https://duckduckgo.com/
  - https://support.google.com/chrome/answer/114836?co=GENIE.Platform%3DDesktop&hl=en
  - https://support.google.com/chrome/answer/114662?co=GENIE.Platform%3DDesktop&hl=en
  - https://brave.com/
  - https://www.mozilla.org/en-US/firefox/

    - https://www.google.com/chrome/browser/desktop/index.html
    - https://myaccount.google.com
- Day 9: Set Up Privacy and Security Extensions in Browser
    - https://www.privacytools.io/
    - https://www.eff.org/https-everywhere
    - https://www.eff.org/privacybadger
    - https://getadblock.com/
    - https://adblockplus.org/
    - https://www.ghostery.com/
    - https://disconnect.me/
    - https://github.com/gorhill/uBlock
- Day 11: Set Up Privacy Conscious Smartphone Apps
    - https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en
    - https://play.google.com/store/apps/details?id=com.whatsapp&hl=en
    - https://play.google.com/store/apps/details?id=org.telegram.messenger&hl=en
    - https://play.google.com/store/apps/details?id=com.brave.browser&hl=en
    - https://play.google.com/store/apps/details?id=com.ghostery.android.ghostery&hl=en
    - https://play.google.com/store/apps/details?id=org.mozilla.focus&hl=en
    - https://play.google.com/store/apps/details?id=org.torproject.android&hl=en
    - https://play.google.com/store/apps/details?id=com.privateinternetaccess.android&hl=en
    - https://play.google.com/store/apps/details?id=com.tunnelbear.android&hl=en
- Day 12: Set Up A Privacy Friendly Cloud Backup Solution
    - https://spideroak.com/one/
    - https://www.sync.com
    - https://tresorit.com/
    - https://www.odrive.com
- Day 13: Set Up A Password Manager
    - https://lastpass.com/f?5074626
    - https://1password.com/
    - https://keepass.info/
    - https://www.dashlane.com/
- Day 14: Generate New Passwords For All Of Your Online Accounts
    - https://knowem.com/
    - https://justdelete.me/
- Day 15: Set Up Two Factor Authentication
    - https://www.yubico.com/
    - https://2fa.directory/
    - https://authy.com/
    - https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en
    - https://play.google.com/store/apps/details?id=com.duosecurity.duomobile&hl=en
    - https://duo.com/
- Day 16: Set Up A VPN
    - https://thatoneprivacysite.net/
    - https://torrentfreak.com/
    - https://www.privateinternetaccess.com/
    - https://www.tunnelbear.com/
- Day 17: Clean Out Your Friends Lists
    - http://justdelete.me/

- Day 18: Go Through Third Party App Permissions and OAuth Services
  - https://myaccount.google.com/permissions
  - http://www.facebook.com/settings/?tab=applications
  - http://twitter.com/settings/applications
  - Update: https://www.cnet.com/how-to/how-to-remove-app-connections-on-linkedin/
  - https://instagram.com/accounts/manage_access
  - https://account.live.com/Consent/Manage
  - Update: https://www.email-support-desk.com/remove-third-party-apps-access-yahoo.html
  - https://www.dropbox.com/account#applications
- Day 19: Clean Up Social Network Privacy Pt 1: Twitter, Snapchat, Youtube, Google
  - https://aboutme.google.com/
  - https://myaccount.google.com/privacycheckup
- Day 20: Clean Up Social Network Privacy Pt 2: Facebook, Instagram, LinkedIn, Other Accounts
  - https://www.facebook.com/settings/?tab=privacy
  - https://www.facebook.com/about/basics
  - https://www.instagram.com/accounts/edit/
- Day 21: Create An Account on Have I Been Pwned
  - http://haveibeenpwned.com/
- Day 22: Email Privacy and Security
  - https://protonmail.com/
- Day 23: Set Up a PGP Private / Public Key Pair
  - https://keybase.io/
- Day 24: How to Spot a Phishing Email or Fake Facebook Page
  - Real: https://www.facebook.com/Disneyland/?ref=br_rs
  - Fake: https://www.facebook.com/Disneyland-California-Adventure-199749506730967/
- Day 25: Spot Fake Support Calls / Social Engineering Attacks
  - https://support.microsoft.com/en-us/contactus/?ws=support
  - https://www.microsoft.com/en-us/reportascam/
  - https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams
- Day 26: Spot ATM Skimmers / Freeze Credit History
  - https://krebsonsecurity.com/all-about-skimmers/
  - https://consumersunion.org/research/consumers-unions-guide-to-security-freeze-protection-2/
  - Equifax — 1-800-349-9960
  - Experian — 1-888-397-3742
  - TransUnion — 1-888-909-8872
  - Innovis — 1-800-540-2505
- Day 27: Opt Out of Public Database Information
  - https://tisiphone.net/2017/01/25/thwart-my-osint-efforts-while-binging-tv/
  - https://joindeleteme.com/
  - https://www.abine.com/blog/2017/how-to-delete-things-from-the-internet/
  - https://www.abine.com/optouts.php
  - http://www.crashoverridenetwork.com/resources.html
- Day 28: Invest in a Faraday Bag / RFID Blocking Wallet / Purse
  - http://amzn.to/2yyBYGo
  - http://amzn.to/2zgq1Co
- Day 29: Upgrade to a Privacy Friendly Operating System / Change OS Settings
  - https://support.apple.com/guide/safari/privacy-preferences-sfri35610

    - https://en.wikipedia.org/wiki/Security-focused_operating_system
- Recommended Blog Reading:
    - https://tisiphone.net/2017/02/08/is-digital-privacy-a-privilege-of-the-wealthy/
    - https://tisiphone.net/2017/01/25/thwart-my-osint-efforts-while-binging-tv/
    - https://decentsecurity.com/#/holiday-tasks/
    - https://medium.com/be-secure/securing-mac-os-x-90137aac6144
    - https://lifehacker.com/the-privacy-enthusiasts-guide-to-using-android-1792432725?utm_campaign=socialflow_lifehacker_twitter&utm_source=lifehacker_twitter&utm_medium=socialflow
    - https://lifehacker.com/how-to-secure-your-online-accounts-by-revoking-access-f-1794631133
    - https://lifehacker.com/roll-your-own-unroll-me-with-a-google-script-1794606005
    - https://www.wired.com/2017/05/spring-clean-digital-clutter-protect/
    - https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/
    - https://arstechnica.com/information-technology/2016/12/a-beginners-guide-to-beefing-up-your-privacy-and-security-online/
    - https://www.theverge.com/2017/6/17/15772142/how-to-set-up-two-factor-authentication
    - https://www.cnet.com/videos/keep-hackers-and-friends-from-using-your-hulu-and-netflix-accounts/
- Security Overviews:
    - https://www.dhs.gov/stopthinkconnect-toolkit
    - https://securityinabox.org/en/
    - https://ssd.eff.org/en
    - http://www.crashoverridenetwork.com/resources.html

Course Outline

Note that you have to sign up for each individual class online.

Date	Start Time	Stop Time	Description
Monday, April 26	6:00 PM	8:00 PM	Security Challenge Kickoff Week 1 Preview (Security Challenge Day 1 - Day 7) 1. Setting Intentions; Inventorying your Accounts & Devices 2. Deleting Old Accounts & Wiping Old Devices **3. Protect your Network & Create a Guest Network** 4. Internet of Things (IoT) Security 5. Setting up Encryption, Lock Screens, FindMyDevice & Auto-Updating 6. Turn off Bluetooth, NFS, wireless 7. Antivirus and Antimalware
Saturday, May 1	12:00 PM	3:00 PM	Weekend Workshop: Securing your Home Wifi ● secure and insecure home wifi configurations ● what is remote administration ● How and why to update your home router ● Benefits of guest networks ● Universal Plug & Play ● Tunnelling DOs and DON'Ts ● Wifi naming techniques ● Optimal router placement ● Introduction to DDWRT and TomatoUSB
Monday, May 3	6:00 PM	8:00 PM	Week 1 Recap, Q&A (Day 1 - Day 7) Week 2 Preview (Day 8 - Day 15) 8. Time for a Better Browser 9. Set up Privacy and Security Extensions 10. Using Proper Internet Hygiene 11. Set up Privacy Conscious Smartphone Apps 12. Set up a Private Cloud Backup Solution 13. Set up a Password Manager 14. Generate New Passwords for All You Online Accounts 15. Set up Two Factor Authentication
Monday, May 10	6:00 PM	8:00 PM	Week 2 Recap, Q&A (Day 8 - Day 15) Week 3 Preview (Day 16 - Day 22) **16. Set up a VPN** 17. Clean Out Your Friends Lists 18. Go Through Third Party App Permissions & OAuth Services 19. Set up Social Network Privacy: Twitter, Snapchat, YouTube, Google 20. Set up Social Network Privacy: Facebook, Instagram, LinkedIn, Other Accounts

			21. Create an Account on HaveIBeenPwned (HIBP) 22. Email Privacy and Security
Saturday, May 15	12:00 PM	3:00 PM	Weekend workshop: Everything you ever wanted to know about VPNs ● Different VPN providers and their tradeoffs ● The process of setting up a VPN on Windows, Mac OS X, iOS, Android, and routers ● Differences between VPNs, Proxies, Tunnels, and Tor ● Free vs. Paid VPNs ● Privacy/anonymity controls ● Preventing malicious traffic ● Log retention policies ● ‘Killswitch’ technology
Monday, May 17	6:00 PM	8:00 PM	Week 3 Recap, Q&A (Day 16 - Day 22) Week 4 Preview (Day 23 - Day 30) 23. Set up PGP Private/Public Keypair 24. How to Spot Phishing Email 25. Spot Fake Support Calls / Social Engineering Attacks 26. Spot ATM Skimmers / Freeze Credit **27. Opt Out of Public Databases** 28. Invest in a Faraday Bad / RFID Wallet/Purse 29. Upgrade to a Privacy Friendly OS 30. Review
Saturday, May 22	12:00 PM	3:00 PM	Weekend workshop: Properly Opting out of Public Databases ● The ecosystem of public databases (e.g. Spokeo, Truth Finder, etc…) ● The laws that govern your personal/private data ● How do find your personal information online, i.e. Googling yourself ● Prerequisites for getting started ● Tracking your progress
Monday, May 24	6:00 PM	8:00 PM	Week 4 Recap, Q&A (Day 23 - Day 30)