How Hackers Hack

or

Hacked People Tell No Tails

by Dr. Vitaly Ford

Arcadia University, office: Boyer Hall 328, vford.me

#EverythingIsHackable
What is the weakest link in cybersecurity?
Hacking Techniques

Gain Trust/Curiosity

or

Incur Fear
Trust but Verify
LinkedIn Job Listing? Gotcha!

That LinkedIn Job Listing May Be a Phishing Scam

Do not give out sensitive information. Anywhere.
T-Mobile?.. RIP

Data on 50M people is leaked

- SSN
- Driver license
- Account PINs

Have you been hacked? Let’s see…

https://haveibeenpwned.com
Passwords? Who uses them anyway…

- **Tr0ub4dor & $**: 28 bits of entropy. Difficulty to guess: easy. Difficulty to remember: hard.
- **Correct horse battery staple**: 44 bits of entropy. Difficulty to guess: hard. Difficulty to remember: you’ve already memorized it.

Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Cracking 12 Character and Above Passwords

https://www.netmux.com/blog/cracking-12-character-above-passwords
Password Managers to the Rescue!

https://bitwarden.com

and please, STOP saving passwords in your browser!
Annoying popup ads?
Too many ads on YouTube?

uBlock Origin plugin

https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamej dnhcphjbkeiagm?hl=en
Dark Search Engine for... everything

https://www.shodan.io

https://www.exploit-db.com/google-hacking-database
Rubber Ducky! Wait, what?

https://youtu.be/sbKN8FhGnqg
Danger Drone, the Real Dark Knight

https://www.youtube.com/watch?v=iG7hUE2BZzo&t=415s
Social Engineering: Best Hack

https://youtu.be/lc7scxvKQOo?t=20
Free Wi-Fi?
10 Airports You Can Easily Get Hacked

https://www.cnbc.com/2018/07/17/these-are-the-10-airports-where-youre-most-likely-to-be-hacked.html
VPN to the Rescue!

https://www.privateinternetaccess.com/
Car Hacking


Garage Hacking

https://samy.pl/opensesame

https://youtu.be/iSSRaIU9_Vc?t=11
Phishing

• UPS phish:


• Buying fake or free domains
But I have an anti-virus!

Look up

“antivirus evasion”

and

“bypass antivirus”

on GitHub.com
Spear-Phishing!

• Open-Source Intelligence (OSINT)
  • https://www.truepeoplesearch.com/
  • Social media profiles
Advanced Phish

• *Curiosity*: Company email

• *Fear*: Ransom
What to do: Emails

• Turn off image loading by default (look it up for your specific service)
• Do NOT click on any link
  • Instead, navigate to the service in question yourself in the browser
• Do NOT open attachments
  • If you are curious, you can download them and then upload to VirusTotal.com
• Curious about a specific website?
  • Enter it to https://urlscan.io or VirusTotal.com
Is 2-FA any good? It depends…

• Modlishka/Evilginx2 tools:

https://vimeo.com/308709275
SMS as a 2-FA? Ugh... give me a break

‘cause:

SIM Swapping
Services that transfer phone numbers
SS7 exploitation
Use App Authenticators
Installing new apps?

I ALSO

LIKE TO LIVE DANGEROUSLY

But Apple users are safe?!.. – LOL

Emails reveal 128 million iOS users were affected by ‘XcodeGhost’ malware

Filipe Espósito - May 7th 2021 1:56 am PT  🌐 @filpeesp sito

https://9to5mac.com/2021/05/07/emails-reveal-128-million-ios-users-were-affected-by-xcodeghost-malware/
Do NOT install new apps unless it’s proven that they are legit
Privacy and Social Media…

Think before Posting
Capture The Flag Competitions

- https://ctftime.org/
- https://www.nationalcyberleague.org/
Learn, Repeat, Profit

• PicoCTF write-up: https://s0cket7.com/picoctf-web/
• Crash Course in CS:
  https://www.youtube.com/playlist?list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo
• All google resources to learn coding and CS, especially for high school & middle school:
  https://edu.google.com/computer-science/?modal_active=none
• Breaking into the power grid: https://www.youtube.com/watch?v=pL9q2lOZ1Fw&t=1s
• Awesome Hacking:
  https://github.com/Hack-with-Github/Awesome-Hacking/blob/master/README.md
• News:
  • https://www.reddit.com/r/netsec/
  • https://krebsonsecurity.com/
  • https://www.wired.com/category/threatlevel/
  • https://news.ycombinator.com/
• Free cybersecurity learning: https://www.cybrary.it/
Learn, Repeat, Profit

• Security cheat sheets: [https://highon.coffee/blog/](https://highon.coffee/blog/)
• Awesome offensive security: [https://github.com/enaqx/awesome-pentest](https://github.com/enaqx/awesome-pentest)
• Different Hacking Environments: [https://github.com/joe-shenouda/awesome-cyber-skills](https://github.com/joe-shenouda/awesome-cyber-skills)
• Make your own lab:
  - [https://github.com/rapid7/metasploitable3](https://github.com/rapid7/metasploitable3)
  - [https://metasploit.help.rapid7.com/docs/metasploitable-2](https://metasploit.help.rapid7.com/docs/metasploitable-2)
  - I would recommend setting up a few virtual machines and go over exploiting those. For instance, you can set up Metasploitable3 ([https://github.com/rapid7/metasploitable3](https://github.com/rapid7/metasploitable3)) and Kali Linux ([https://www.kali.org/downloads/](https://www.kali.org/downloads/)), then look into videos on youtube like [https://www.youtube.com/playlist?list=PLZOToVAK85MpnipcVtNMwmCxMZRPFaY6mT](https://www.youtube.com/playlist?list=PLZOToVAK85MpnipcVtNMwmCxMZRPFaY6mT) and you can follow along and see the process of pentesting.
Trust but **Verify**

and please, **become “paranoid”**

about your security
In Doubt? Contact Dr. Soviet (aka Vitaly Ford)

Boyer Hall 328 (near the elevator)

fordv@arcadia.edu

https://vford.me