

How Hackers Hack or Hacked People Tell No Tails

by Dr. Vitaly Ford

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

[#EverythingIsHackable](https://twitter.com/EverythingIsHackable)

What is the weakest link in
cybersecurity?

Hacking Techniques

Gain Trust/Curiosity
or
Incur Fear

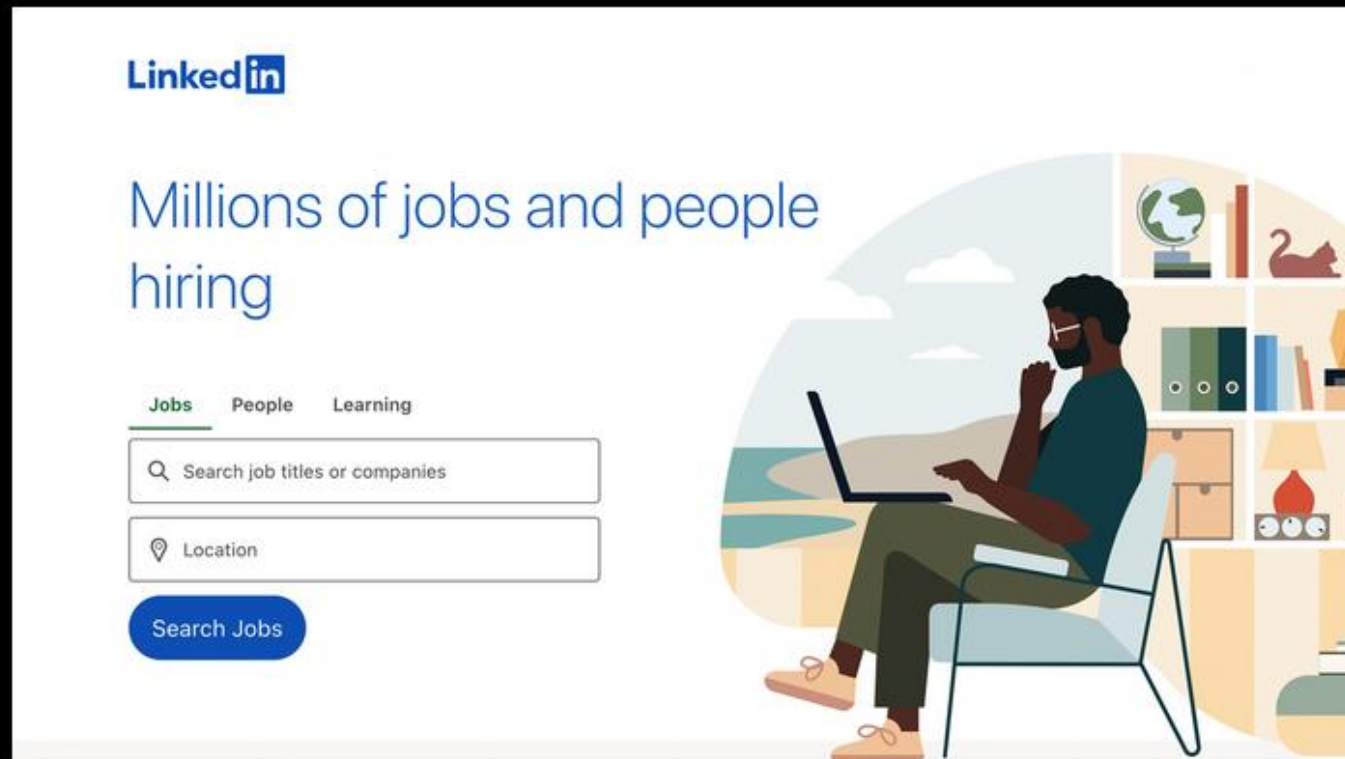
Trust but Verify


LinkedIn Job Listing? Gotcha!

That LinkedIn Job Listing May Be a Phishing Scam



ANDREW HEINZMAN  @andrew_andrew__
AUG 20, 2021, 11:17 AM EDT | 1 min read



 LinkedIn

Do not give out sensitive
information. Anywhere.

T-Mobile?.. RIP

Data on 50M people is leaked

- SSN
- Driver license
- Account PINs

T-Mobile data breach and SIM-swap scam: How to protect your identity

Even if you're not a T-Mobile customer, SIM-swap fraud is real. Here are some ways you can avoid it.



Jason Cipriani Aug. 22, 2021 6:30 a.m. PT

LISTEN - 06:11



37



SIM swapping is when a scammer transfers your phone number to another device to access your accounts.

Jason Cipriani/CNET

Have you been hacked? Let's see...

<https://haveibeenpwned.com>

Passwords? Who uses them anyway...

XKCD

The comic strip is divided into six panels. The top row contains three panels, and the bottom row contains three panels. The bottom-most panel is a wide text box.

Top Row, Panel 1: A diagram showing the construction of the password "Tr0ub4dor &3". It is categorized as "UNCOMMON (NON-GIBBERISH) BASE WORD" and "ORDER UNKNOWN". Annotations include "CAPS?", "COMMON SUBSTITUTIONS", "NUMERAL", and "PUNCTUATION". A note at the bottom says: "(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)".

Top Row, Panel 2: States "~ 28 BITS OF ENTROPY" and " $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$ ". A note in parentheses says: "(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)". Below it, "DIFFICULTY TO GUESS: EASY".

Top Row, Panel 3: A character asks, "WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?" and "AND THERE WAS SOME SYMBOL...". Below it, "DIFFICULTY TO REMEMBER: HARD".

Bottom Row, Panel 1: A diagram showing the password "correct horse battery staple". It is categorized as "FOUR RANDOM COMMON WORDS".

Bottom Row, Panel 2: States "~ 44 BITS OF ENTROPY" and " $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$ ". Below it, "DIFFICULTY TO GUESS: HARD".

Bottom Row, Panel 3: A character thinks, "THAT'S A BATTERY STAPLE." and "CORRECT!". Below it, "DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT".

Bottom Panel: A wide text box containing the text: "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/cjpalhdlnbpafiamejdnhcphjbkeiagm?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

<https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/>

<https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/>

<https://nakedsecurity.sophos.com/2018/11/30/driver-loses-his-car-to-hackers-twice/>

Garage Hacking

<https://samy.pl/opensesame>

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

Phishing

- UPS phish:

<https://www.bleepingcomputer.com/news/security/phishing-campaign-uses-upscom-xss-vuln-to-distribute-malware/>

- 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

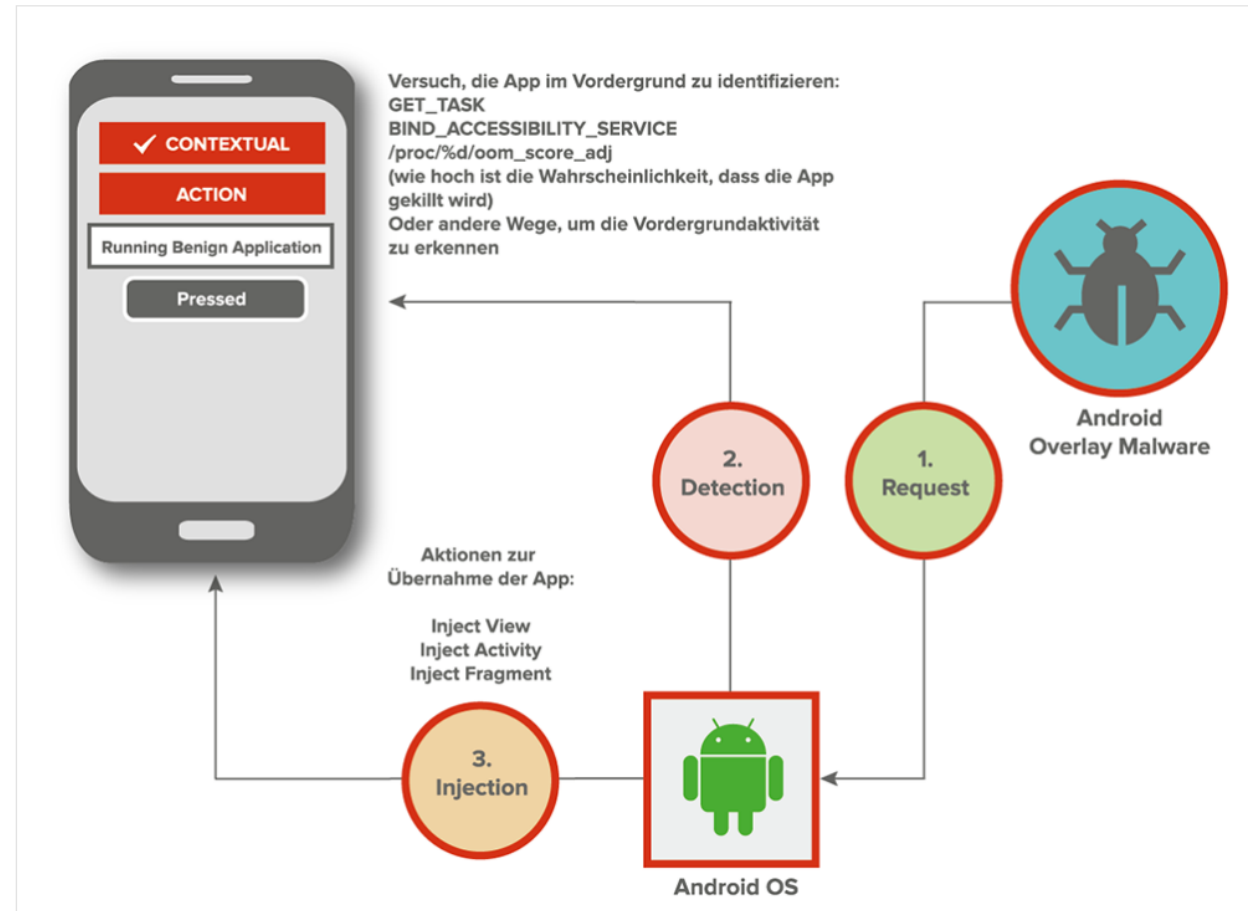
SS7 exploitation

Use App Authenticators

Installing new apps?



1. Picking a victim application and finding out their package name
2. Monitoring said application using various methods
3. Hijacking hijacking the victim App by overlaying it at run time.



But Apple users are safe?!.. – LOL

Emails reveal 128 million iOS users were affected by 'XcodeGhost' malware

Filipe Espósito - May. 7th 2021 1:56 pm PT [@filipeesposito](#)



Do NOT install new apps

unless it's proven that they are legit

Privacy and Social Media...

<https://www.bbc.com/news/technology-46456695>

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=PL8dPuuaLjXtNIUrzyH5r6jN9ulIgZBpdo>
- 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/>
- Awesome offensive security: <https://github.com/enaqx/awesome-pentest>
- Different Hacking Environments: <https://github.com/joe-shenouda/awesome-cyber-skills>
- Make your own lab:
 - <https://github.com/rapid7/metasploitable3>
 - <https://metasploit.help.rapid7.com/docs/metasploitable-2>
 - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
 - 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>) and Kali Linux (<https://www.kali.org/downloads/>), then look into videos on youtube like <https://www.youtube.com/playlist?list=PLZOToVAK85MpnjpcVtNMwmCxMZRFaY6mT> 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>