Forum Donate

Learn to code — free 3,000-hour curriculum

JUNE 6, 2023 / #CYBERSECURITY

How Hackers Attack Social Media Accounts – And How to Defend Against Them

Daniel Iwugo

Hey everyone, and welcome to the world of Social Media 📲.

In this article, we will explore the famous (or infamous) sphere of social media, why it is critical to both you and hackers, and how you can avoid having your social media accounts attacked.

Disclaimer: Hacking is a tool with the potential for both good and bad. Under no circumstances should the knowledge in this article be used for any harmful or illegal purposes. Doing so could lead to a long time in a jail cell 💀.

And with that, let's jump in 🙃.

What We'll Cover

1. Overview of Social Media Platforms
2. Attack Techniques

Forum Donate

Learn to code — free 3,000-hour curriculum

Overview of Social Media Platforms

Media is Everything ¦ Credit: Anledry Cobos

Meta (formerly Facebook) remains one of the biggest companies on the planet.

Starting off in 2004, it redefined the way we interact with, share, and engage with the world around us. With roughly 2.98 billion monthly active users, Facebook has become an integral part of modern society, bridging gaps and fostering virtual communities.

The platform was among the pioneers of the social media craze which introduced the world to more apps such Instagram, Snapchat, Reddit, WhatsApp, YouTube, TikTok, Telegram and most notoriously, Twitter . Each and every single one of these apps

Forum Donate

Learn to code — free 3,000-hour curriculum

Connections to people, places and products have been the centre of it all. These platforms allow you to interact with friends, as well as strangers. They also help you see the world around you in ways no one thought was possible many years ago. And if you're a business person or content creator like I am, it allows you to show people what you have to offer.

If an attacker compromises your credentials, they have access to your connections. They could use your data to impersonate you, post illegal and harmful things, damage your reputation, spread malware, and social engineer your friends and followers on the platform in order to steal money and compromise their accounts.

According to Gitnux, there are about 1.4 billion attacks on social media platforms monthly – quite a lot isn't it?

Forum Donate

Learn to code — free 3,000-hour curriculum

Giga Chad ¦ Credit: The Hacker Community

Many companies take the cybersecurity of their infrastructure quite seriously (most times anyway 😮). But as a consumer, you are your own last line of defense or your own greatest vulnerability.

In this article, we will take a look at some ways attackers can convert your 'connections' into profit and how you can defend against them. Now let's find out how hackers can compromise your account.

Social Media Account Attack Techniques

Forum Donate

Learn to code — free 3,000-hour curriculum

A 'Like' signboard on 1 Hacker Way ¦ Credit: Greg Bulla

Physical Access

This may seem obvious, but people still make this mistake a lot. An attacker could install scripts or software that would let them get the passwords of your social media accounts if they have your phone or laptop in their hand.

Software like those from Passrevelator make it easy to get passwords and other credentials from devices on different platforms.

Here's a screenshot from one of them, Pass Wi-Fi, below. This one gets all SSIDs and passwords the device has ever connected to.

Forum Donate

Learn to code — free 3,000-hour curriculum

Pass Wi-Fi in action ¦ Credit: Passrevelator

Phishing links, emails, and sites

Phishing is a cyberattack in which the attacker tricks the victim into giving sensitive or critical information through fraudulent websites, forms, links or other means.

It's pretty easy for anyone to make a Facebook clone with React Native. Tools like Zphisher and PyPhisher make it even easier for an attacker by setting up a phishing page and creating links to it, too.

As you can see, PyPhisher comes with a wide array of options for some major mayhem.

Forum Donate

Learn to code — free 3,000-hour curriculum

The Phyphisher Interface ¦ Credit: Mercury

More seasoned criminals can send links in spoofed emails to make them look like they are from official organisations and can register lookalike domains to trick users.

Password Spraying and Bruteforcing

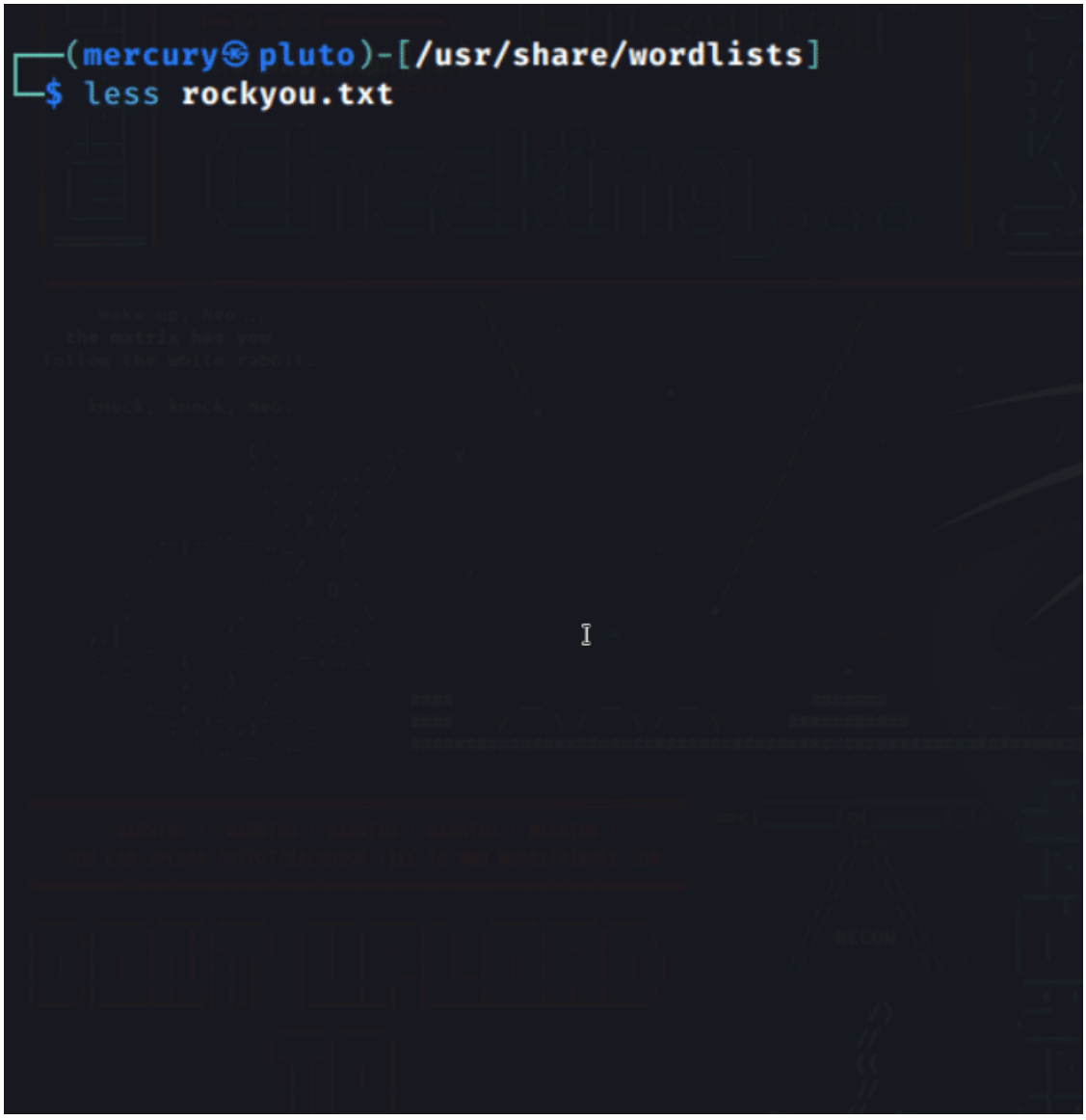
Passwords are a big security concern, and for good reason. They are often repetitive and easy to guess. Spraying is the process of trying out common passwords while Bruteforcing is the process of trying out all possible combinations to gain access.

Attackers can get the passwords they use in password spraying from common **wordlists**. Wordlists are a list of passwords usually

Forum Donate

Learn to code — free 3,000-hour curriculum

Below is a screenshot of the infamous rockyou.txt wordlist from the RockYou hack of 2009.



The rockyou.txt wordlist ¦ Credit Mercury

Bruteforcing, on the other hand, involves the attacker generating a custom wordlist alongside usernames or emails on different platforms. This is more effective if the attacker has a specified target.

Forum Donate

Learn to code — free 3,000-hour curriculum

Crunch in action ¦ Mercury

If an attacker uses these techniques on a login page, this has great potential to be an entry point, especially if the site has poor security.

Keyloggers

A Keylogger is a piece of riskware that keeps track of what a person types on their device. Think of it like your keyboard having a memory card and sending what it stores to an attacker.

Note that keyloggers aren't inherently bad, as they can also be used for organisational monitoring and parental control. But an attacker does not have authorization to monitor your keystrokes, which makes its use illegitimate.

An attacker could install a keylogger and monitor the victim's keystrokes. All they have to do is wait and read the logs for a peculiar sequence, usually one with an email, followed by a string of characters before the 'return' keystroke.

Forum Donate

Learn to code — free 3,000-hour curriculum

A slightly modified Keylogger log ¦ Credit: Mercury

Usually, the entire log will be monochrome but for this example I made a few modifications. The red highlight indicates an email account, which is what an attacker would be looking for. Close behind is the password in blue.

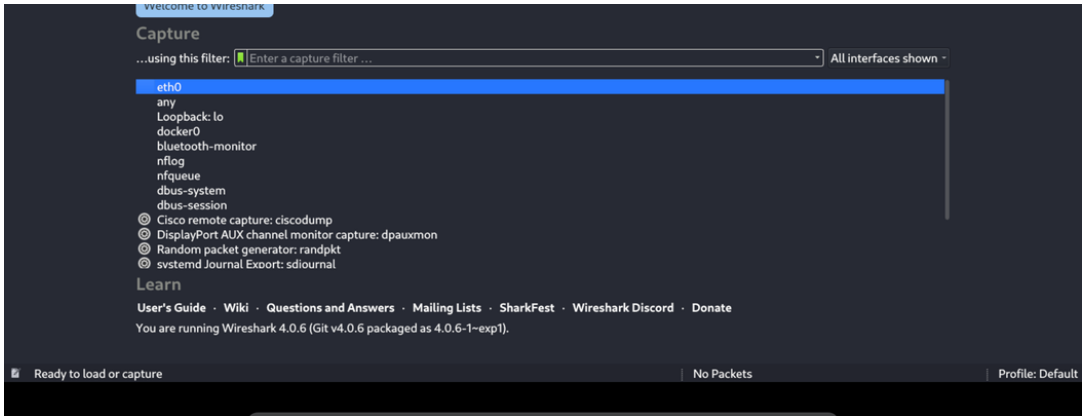
Network Sniffing

Also known as packet sniffing, this is the practice of intercepting and analysing network packets in order to find out what kind of information is shared within the network.

If connections are not properly encrypted, an attacker could easily obtain sensitive information about the sites visited and the messages and passwords that are sent and inputted in them, respectively. WireShark is one of the most common tools for this kind of attack.

Forum Donate

Learn to code — free 3,000-hour curriculum



The Wireshark Interface ¦ Credit: Mercury

Data Breaches

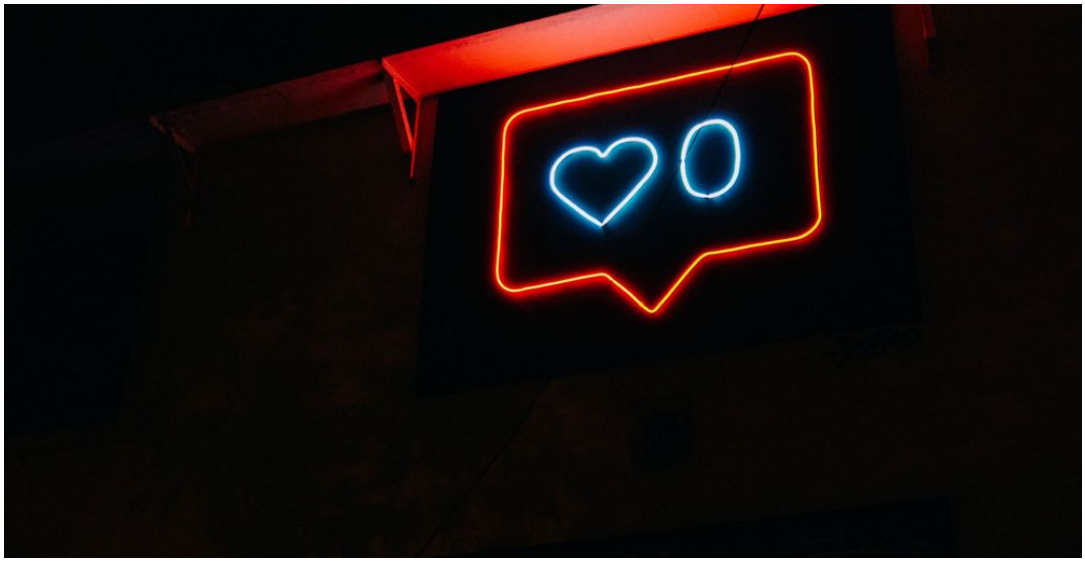
Data breaches are unintentional leaks of sensitive or confidential information. These are usually more devastating to users than organisations and could have far-reaching consequences.

Passwords and login credentials from data leaks can be sold and purchased on the dark web. They are then used to gain unauthorised access to the account and the rest is history.

How to Defend Against Social Media Attacks

Forum Donate

Learn to code — free 3,000-hour curriculum



A Neon Instagram Heart ¦ Credit: Prateek Katyal

As you can see, there are many ways to obtain Social Media account credentials. Below are some ways to ensure you are not a victim.

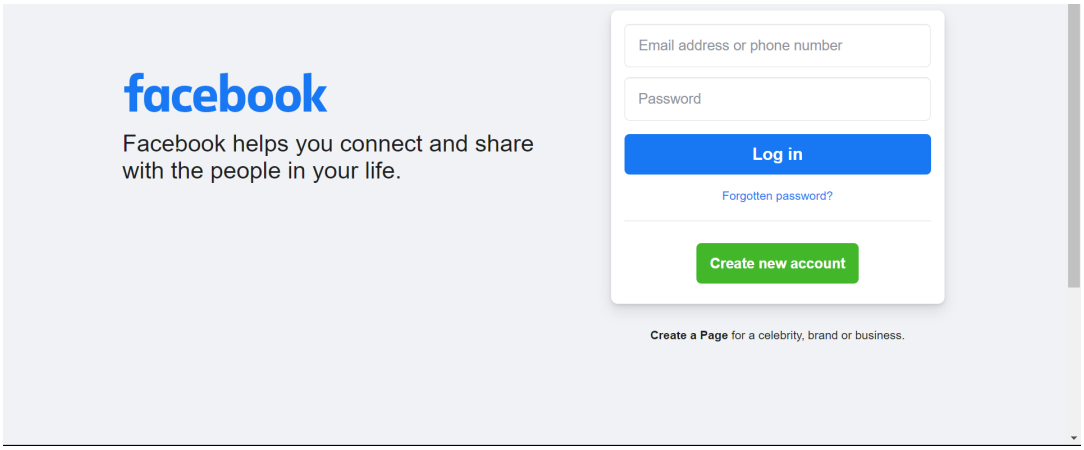
Check the URL

Always double check any links sent to you via messaging platforms or email. This is a simple but very effective measure against phishing links and sites, as the likelihood of clicking on the wrong link is much lower.

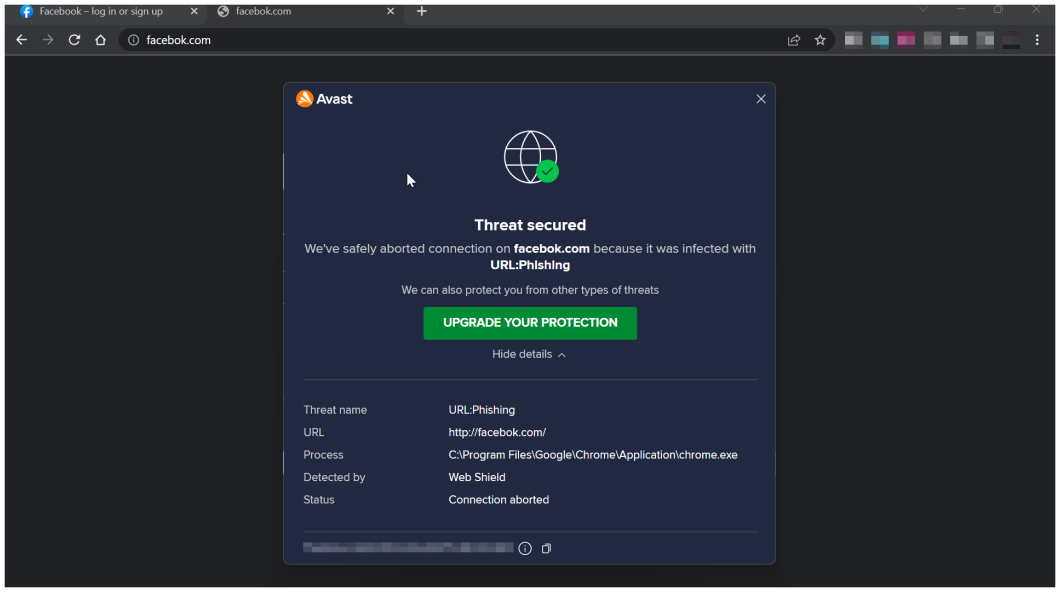
For example, www.facebook.com and www.facebok.com are not the same. As you can observe in the screenshots below, the former is legitimate while an antivirus warns me that the later is a phishing site.

Forum Donate

Learn to code — free 3,000-hour curriculum



facebook.com ¦ Credit: Mercury



facebok.com ¦ Credit: Mercury

Use strong passwords/passphrases

Make sure you use strong passwords and don't use similar passwords for different accounts (not even variants 👀). You can also use passphrases rather than passwords as they are easier to remember but harder to guess or bruteforce.

An example of a password is 'dictionary'. An example of a passphrase is 'mydictionaryisthelargest'. The password is weak and

Forum Donate

Learn to code — free 3,000-hour curriculum

Use Antivirus Software and Firewalls

An Antivirus is a software solution that protects systems against both internal and external threats based on the vendor. A Firewall, on the other hand, protects systems against external threats based on your preferences and settings.

The use of one or both of these products can go a long way in protecting both individuals and organisations from information stealing malware.

VPNs

A Virtual Private Network is a secure network connection that connects you to the internet privately and anonymously. This is done by encrypting the connection and routing it through remote servers.

VPNs are a great option to avoid packet sniffers because packets analysed are encrypted. This means it's going to be quite difficult for an attacker to get passwords from technical gibberish.

Tracking Breaches

Tracking breaches can be done at an individual or enterprise level. It's effectiveness, however, usually depends on how much you are willing to pay for it.

Individuals can use sites like haveibeenpwned.com to check if their data has been compromised in any breaches and Enterprises can

Forum Donate

Learn to code — free 3,000-hour curriculum

Conclusion

Social Media in Scrabble ¦ Credit: Visual Tag Mx

Getting credentials is pretty easy with some determination and a touch of mischievousness. But companies have gotten better at defense in recent years and attackers have had to get more creative.

As an individual, you are your last and dare I say best line of defense. Ensure your shields are always up in the online jungle. Stay safe and Happy Hacking 🙃.

Acknowledgements

Thanks to Anuoluwapo Victor, Chinaza Nwukwa, Holumidey Mercy, Favour Ojo, Georgina Awani, and my family for the inspiration, support and knowledge used to put this together. You're the best.

Forum Donate

Learn to code — free 3,000-hour curriculum

2. GUI tools for physical access hacking

Daniel Iwugo

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet

If you read this far, tweet to the author to show them you care.

Tweet a thanks

Learn to code for free. freeCodeCamp's open source curriculum has helped more than 40,000 people get jobs as developers.

Get started

freeCodeCamp is a donor-supported tax-exempt 501(c)(3) charity organization (United States Federal Tax Identification Number: 82-0779546)

Our mission: to help people learn to code for free. We accomplish this by creating thousands of videos, articles, and interactive coding lessons - all freely available to the public. We also have thousands of freeCodeCamp study groups around the world.

Donations to freeCodeCamp go toward our education initiatives, and help pay for servers, services, and staff.

You can make a tax-deductible donation here.

Trending Guides

Exponents in Python

What is SQL?