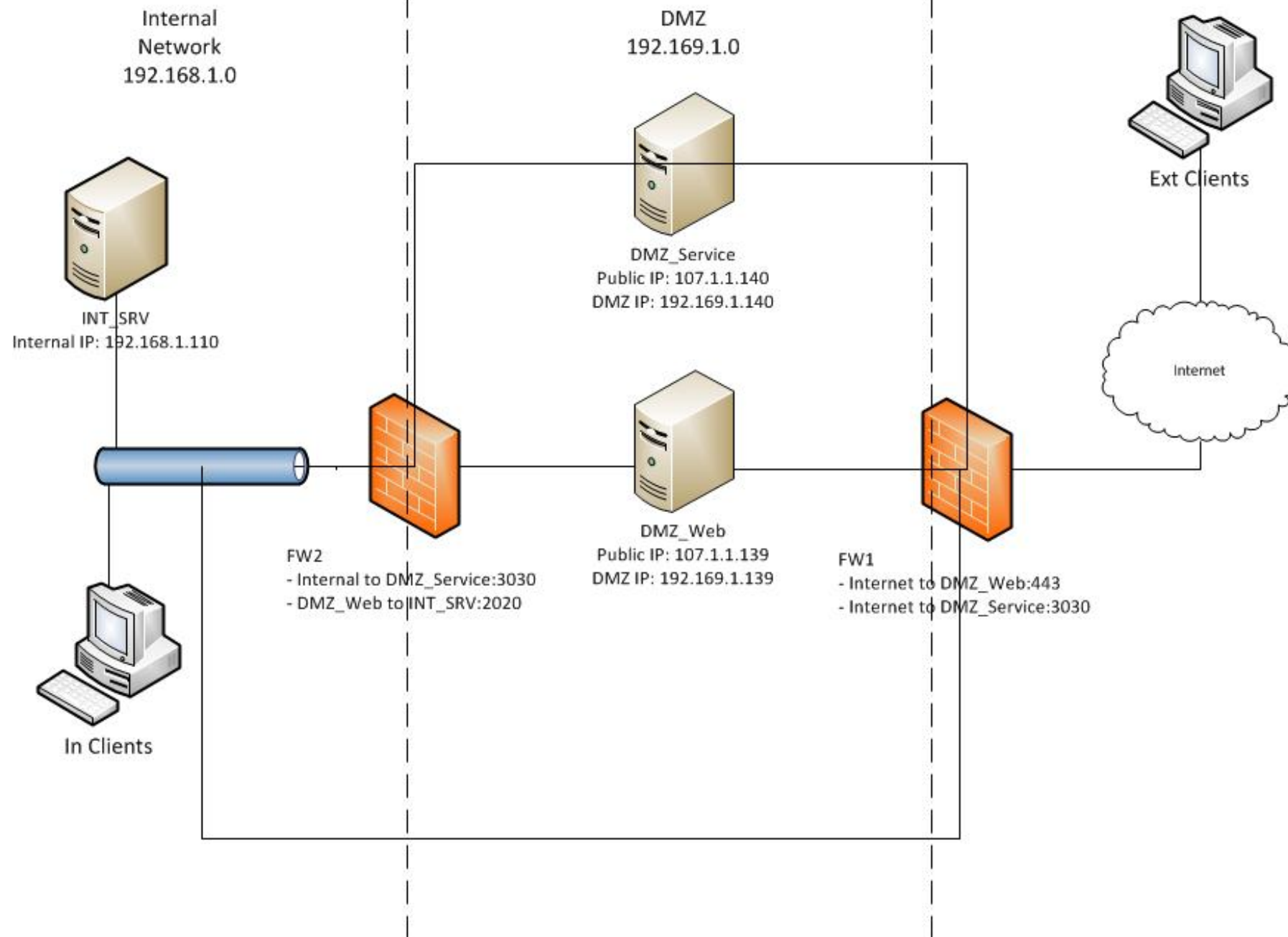IT-Serurity

Stay Secure

- Firewall - **ON**

- Antivirus - **ON**

- HTTPS websites - **ONLY**

- Open Wi-Fi - **NO**

- VPN - **USE**

- Use secure passwords - **USE**

- Password Manager - **USE**

- Two-Factor Authentication - **USE**

Firewall

Internal
Network
192.168.1.0

DMZ
192.169.1.0

Ext Clients

Internet

DMZ_Service
Public IP: 107.1.1.140
DMZ IP: 192.169.1.140

INT_SRV
Internal IP: 192.168.1.110

DMZ_Web
Public IP: 107.1.1.139
DMZ IP: 192.169.1.139

FW2
- Internal to DMZ_Service:3030
- DMZ_Web to INT_SRV:2020

FW1
- Internet to DMZ_Web:443
- Internet to DMZ_Service:3030

In Clients

Antivirus

Common types of cyber threats

-Malware

-Spyware

-Phishing

Malware

Malware, short for *malicious software*, is a blanket term that refers to a wide variety of software programs designed to do damage or do other unwanted actions to a computer, server or computer network Common examples include viruses, spyware and trojan horses.

Malware can slow down or crash your device or delete files.

Criminals often use malware to send spam, obtain personal and financial information and even steal your identity.
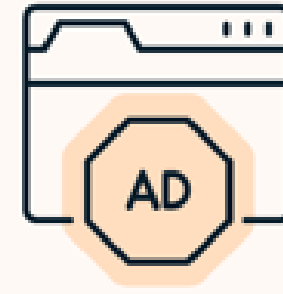
Types of Malware

RANSOMWARE

Blackmails you

SPYWARE

Steals your data

ADWARE

Spams you with ads

WORMS

Spread across computers

TROJANS

Sneak malware onto your PC

BOTNETS

Turn your PC into a zombie

Spyware

Spyware is a type of **malware** that attaches itself and hides on a computer's operating system without your permission to make unwanted changes to your user experience.

It can be used to spy on your online activity and may generate unwanted advertisements or make your browser display certain website sites or search results.

Phishing

Phishing attacks use email or fraudulent websites to try to trick you into providing personal or financial information to compromise an account or steal money by posing as a trustworthy entity.

They may claim there's a problem with payment information or that they've noticed activity on an account and ask you to click on a link or attachment and provide personal information.

How does antivirus work?

Antivirus software begins operating by checking your computer programs and files against a database of known types of malware.

Since new viruses are constantly created and distributed by hackers, it will also scan computers for the possibility of new or unknown type of malware threats.

Most antivirus programs will use three different detection devices

- **Specific detection** - Identifies known malware

- **Generic detection** - Looks for known parts or types of malware or patterns that are related by a common codebase

- **Heuristic detection** - Scans for unknown viruses by identifying known suspicious file structures.

When the antivirus program finds a file that contains a virus, it will usually quarantine it and/or mark it for deletion, making it inaccessible and removing the risk to your device.

HTTPS

HTTPS

Hypertext Transfer Protocol Secure (*HTTPS*) is an extension of the Hypertext Transfer Protocol (*HTTP*).

It is used for secure communication over a computer network, and is widely used on the Internet.

In HTTPS, the communication protocol is **encrypted** using Transport Layer Security (*TLS*) or, formerly, Secure Sockets Layer (*SSL*)
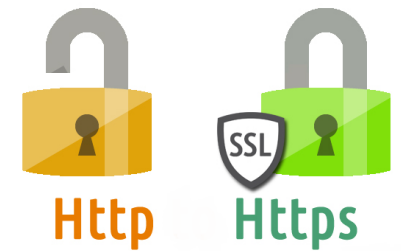
HTTP

When you connect to a website with regular **HTTP**, your browser looks up the IP address that corresponds to the website, connects to that IP address, and assumes it's connected to the correct web server.

Data is sent over the connection in clear text. An eavesdropper on a Wi-Fi network can see the web pages you're visiting and the data you're transferring back and forth.

There's no way to verify you're connected to the correct website. You think you accessed your bank's website, but you're on a compromised network that's redirecting you to an impostor website. Passwords and credit card numbers should never be sent over an HTTP connection, or an eavesdropper could easily steal them.

HTTPS

When you connect to an **HTTPS**-secured server—secure sites like your bank's will automatically redirect you to HTTPS—your web browser checks the website's security certificate and verifies it was issued by a legitimate certificate authority.

This helps you ensure that, if you see *https://bank.com* in your web browser's address bar, you're actually connected to your bank's real website.

The company that issued the security certificate vouches for them.

When you send sensitive information over an HTTPS connection, **no one can eavesdrop on it in transit**. HTTPS is what makes **secure** online banking and shopping possible.

The presence of HTTPS itself isn't a guarantee a site is legitimate.

Clever phishers have realized that people look for the **HTTPS** indicator and lock icon, and may go out of their way to disguise their websites.

Scammers can get certificates for their scam servers, too. In theory, they're only prevented from impersonating sites they don't own. You may see an address like

https://google.com.3526347346435.com

In this case, you're using an **HTTPS** connection, but you're really connected to a subdomain of a site named **3526347346435.com**— **not Google**

Open Wi-Fi

Open Wi-Fi

It's not safe to connect to an unknown open wireless network, particularly when transferring sensitive data, such as an online banking password.

All information sent over an unsecured wireless network—one that doesn't require a Wi-Fi Protected Access (*WPA*) or *WPA2* security code—is sent in plain text for anyone to intercept.

Connecting to an open network potentially opens your device to anyone else on that same wireless network.

VPN

VPN

A **Virtual Private Network** (*VPN*) connects to the internet privately by hiding your *real IP address* and routing your internet traffic and data through a private and securely encrypted tunnel over public networks.

VPN gives you a way to browse the internet without giving away your *identity*, *location*, or *data*.

When data is encrypted inside the VPN tunnel, ISPs, search engines, marketers, hackers, and others can't see or track your activities on the web.

How a VPN works

VPN

User Device — VPN Client — Internet Service Provider — VPN Server — Internet

Encrypted   Encrypted

No VPN

User Device — Internet Service Provider — Internet

EMSISOFT
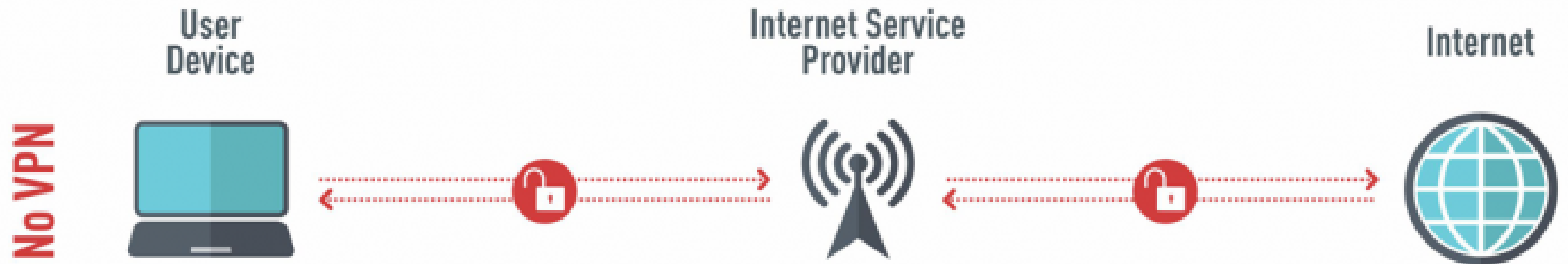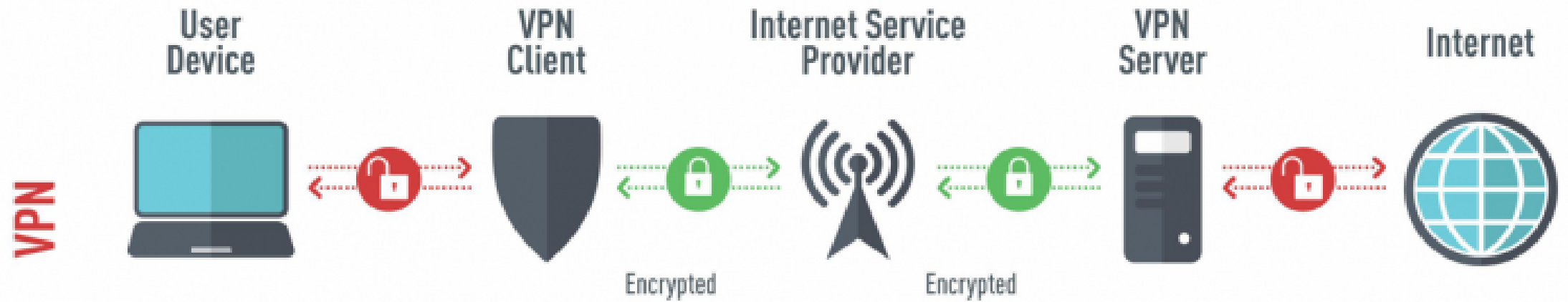
VPNs protect you in three main ways

- **Disguises** your real IP address and location. After connecting to a VPN service, you go to the internet from a new gateway server. This spoofs your IP address and makes it appear as if you're in a different city or country than the one you're in.

- **Encapsulates** your internet traffic through a private VPN tunnel. With a VPN, all your *data packets* are encapsulated inside additional data packets. This encapsulation creates a private tunnel inside public networks.

- **Scrambles** your private data with encryption. When using a VPN service, your internet traffic and personal information inside the tunnel are scrambled using encryption. This makes a VPN connection virtually impossible for outside forces to hack.

Password Security
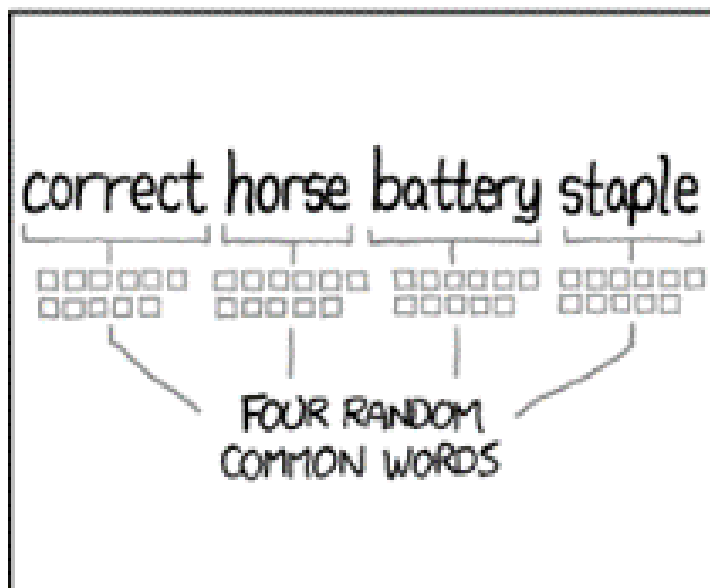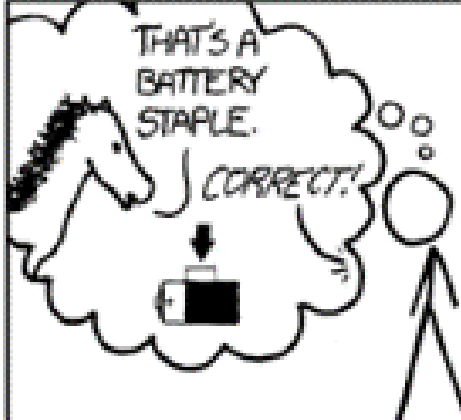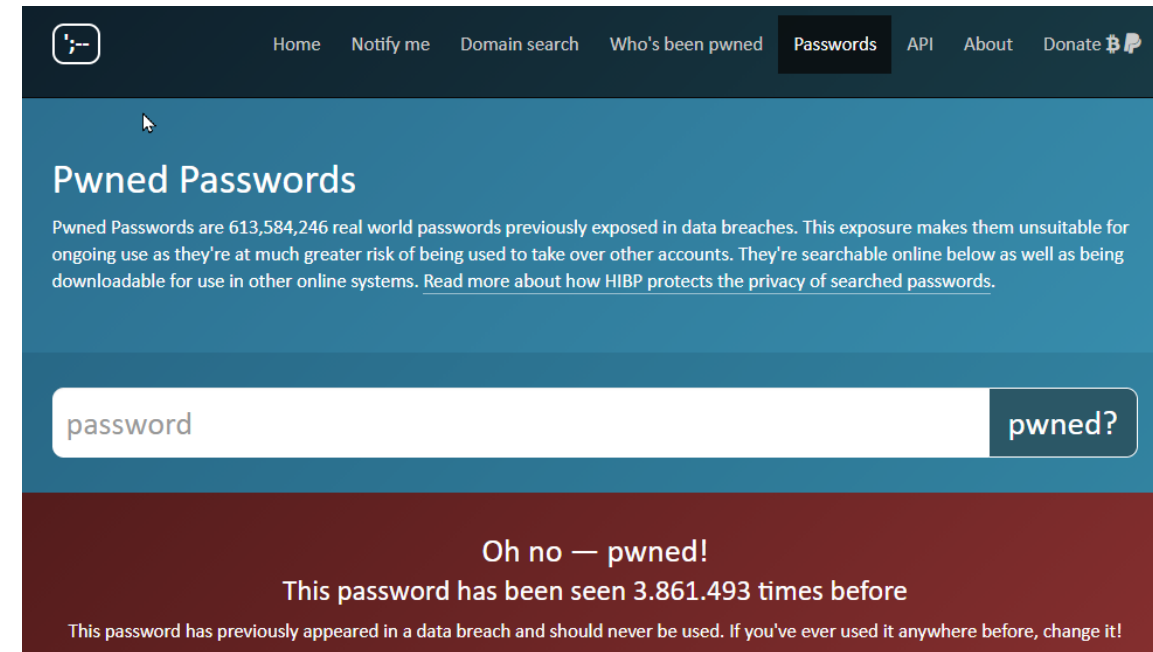
Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.

Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches

https://haveibeenpwned.com/Passwords

Brute-Force attack

Brute-Force attacks (*just trying out all possible combinations*) have become computationally easy => **its simpler to just try out all combinations than to guess something clever**

GitHub

Avoid revealing your passwords on GitHub

- Always keep your password and login information in a **separate file** - *config.ini*
- Use **.gitignore** so you do not sync that files with password and login information to GitHub

Python code

```python
# Imports
import itertools
import time


# Brute force function
def tryPassword(passwordSet, stringTypeSet):
    start = time.time()
    chars = stringTypeSet
    attempts = 0
    for i in range(1, 9):
        for letter in itertools.product(chars, repeat=i):
            attempts += 1
            letter = ''.join(letter)
            if letter == passwordSet:
                end = time.time()
                distance = end - start
                return (attempts, distance)

password = input("Password:")

# Allowed characters
stringType = "1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ`~!@#$%^&*()_-+=[{]}|:;'\",<.>/?"
tries, timeAmount = tryPassword(password, stringType)
print("Cracked the password %s in %s tries and %s seconds!" % (password, tries, timeAmount))
```

```
Password: tue
Cracked the password tue in 262368 tries and 0.048001766204833984 seconds!
```
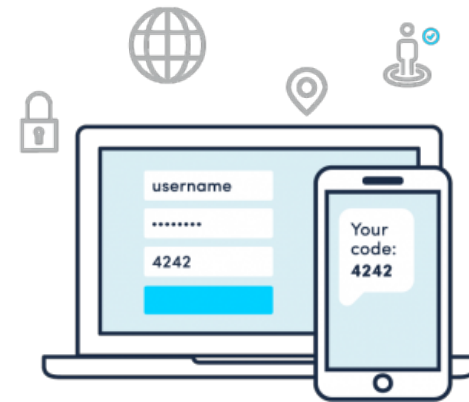
Two-Factor Authentication

Two-Factor Authentication

Logging into your accounts with an email address and password is fine, up to a point, but these details can get lost, stolen, guessed, or teased out of you with some clever social engineering.

Two-factor authentication adds another access barrier for unauthorized visitors who have gotten hold of your primary login credentials

Two-factor authentication—and the similar two-step authentication, which is sometimes treated as a different mechanism and sometimes not—means you need another bit of information besides your password and email address. Most commonly in most consumer apps, it's either an SMS code sent to your phone, or a code generated by a dedicated authenticator app.

Links

Links

- https://www.restapitutorial.com/httpstatuscodes.html#
- http://testphp.vulnweb.com/disclaimer.php
- https://github.com/tanc7/hacking-books/blob/master/Violent Python - A Cookbook for Hackers%2C Forensic Analysts%2C Penetration Testers and Security Engineers.pdf
- https://github.com/mehransab101/Black_Hat_Python/blob/master/Black Hat Python_Python_hacking_for_programmers_and_pentesters.pdf
- https://github.com/l34n/CySecBooks/blob/master/Gray Hat Python - Python Programming for Hackers and Reverse Engineers (2009).pdf