WORKING REMOTELY SECURING YOUR HOME NETWORK

Compiled by Frans Roodt CHFI CEH

What is a Home Network ?

- Connecting an internet access point such as a cable from your internet service provider MWEB, Telkom. To a wireless router in order to allow multiple devices to connect to the network.
- You might also want to extend your home network with a second router in this scenario the settings of the second router must match those of the first. It’s easier to use the same models.
- I’m just going to go over the setup of the primary router I’m using an Asus the location of the settings will differ from one model to the other but the options will be the same.

Secure Router Setup

- I usually use the routers setup wizard and do the rest of the settings afterwards
- The settings SHOULD NOT! Be used as default
- Set your wireless network encryption as WPA2-AES
- Use long and complex passwords, if you can remember a 24 character password that's excellent.

Where to find the setting

After finishing the setup wizard login to your routers login page the step will be the same across all models although the default ip address will differ for an example mine is Http://192.168.1.1

Changing the settings

- The default username and password will usually be Username: admin, and password: admin.
- Or Admin, Password this will differ from one model to another this is the first thing you will need to change

> When you successfully log in to the router's configuration,

> Click Administration under Advanced Settings.

> Click the System tab to change the router login credentials.

> Type your new Router Login Name and New Password.

ASUS RT-N56U

Back main Page

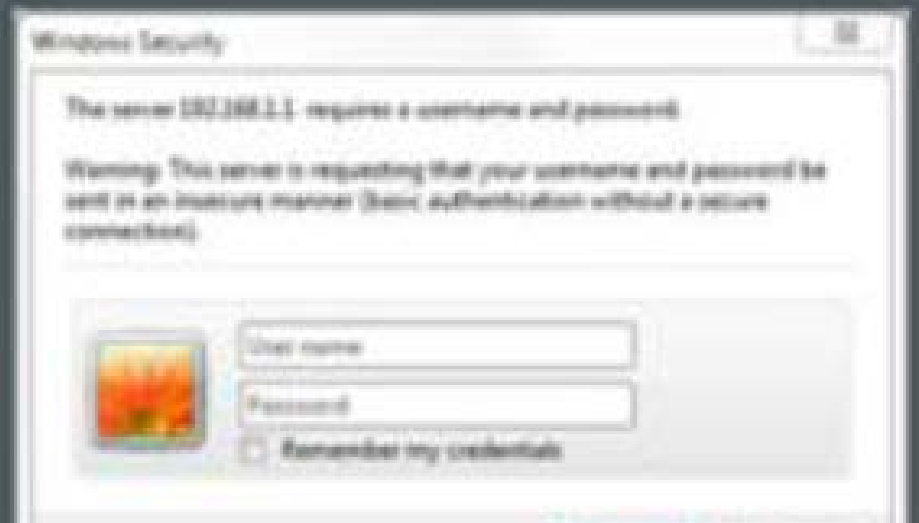
- Quick Internet Setup
- Check Connection
- Internet Setup
- Router Setup

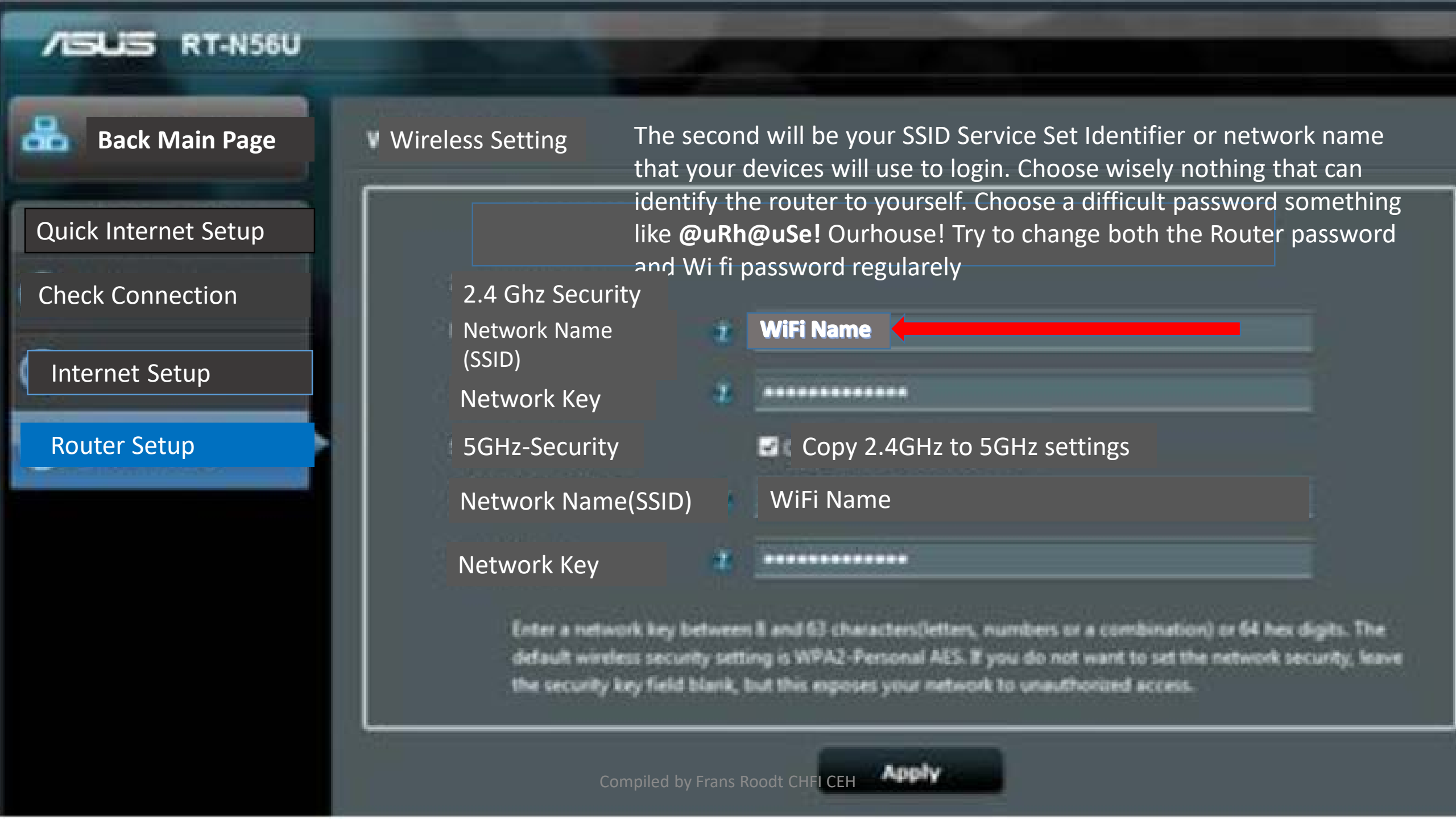
Change the default username and password to prevent unauthorized access to your wireless router don't use your Surname as a clever intruder can easily guess the login name

Router login name	Admin
New Password	•••••••• Very Weak
Retype New Password	••••••••

Show password

The router password is the administration key to your ASUS router. When you log into the router's web user interface, you will need to key in the username and password. The default router username and password is admin / admin Username and password are case sensitive




ASUS RT-N56U
Back Main Page
Quick Internet Setup
Check Connection
Internet Setup
Router Setup
Wireless Setting
The second will be your SSID Service Set Identifier or network name that your devices will use to login. Choose wisely nothing that can identify the router to yourself. Choose a difficult password something like @uRh@uSe! Ourhouse! Try to change both the Router password and Wi fi password regularely
2.4 Ghz Security
Network Name (SSID)
WiFi Name
Network Key
5GHz-Security
Copy 2.4GHz to 5GHz settings
Network Name(SSID)
WiFi Name
Network Key
Apply

After QIS (Quick Internet Setup), the system set WPA2-AES as your default encryption.
Although the system provides multiple encryptions, keep your system in WPA2-AES encryption if there is no special requirement

Set up separate passwords for your wireless network and Web GUI
The web GUI is your routers web login page the 192.168.1.1 we talked about earlier I know two passwords is hard to remember but use imagination.

IMPORTANT!

Update your router to the latest firmware

Some routers do this part automatically on other models the update needs to be done manually please check your router manual on how to do this.

Enable the firewall

Firewall setting page is in Advanced Settings. The default value is enabled. Please do not disable the firewall if there is no special requirement.

Disable the access from WAN

Access from WAN allows you to access your router from the Internet. The default value of this function is disabled. Do not enable this function if there is no special requirement. Visit Advanced Settings-> Administration -> Remote Access Config for configuration. On Asus Routers

- That is the very basic settings for getting your router secured however there are more advanced settings that can be activated please refer to your router manual for this.
- Another common router is the TP-Link TD-W8961N as this is one of the cheaper routers but more complicated to setup a quick explanation on changing the default router password
- To reset the admin password of your TP-LINK router

- Open web browser and type the IP address of the wireless router in the address bar, and press Enter. The default IP address of TP-Link router is 192.168.1.
- Type the username and password in the login page. The default username and password are both admin in lowercase.
- Click Management->Access Control->Password on left page, and type the old password and new password.
- Click Save/Apply to save the settings.

- **To reset the Wi-Fi password of your TP-LINK router**

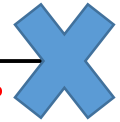
- Open web browser and type the IP address of the wireless router in the address bar, and press Enter. The default IP address of TP-Link router is 192.168.1.
- Type the username and password in the login page. The default username and password are both admin in lowercase.
- Click Wireless on the left side of the page
- Click Wireless Security. This option is below the Wireless menu on the left side of the page.
- Scroll down and check the WPA-PSK/WPA2-PSK box. It's near the bottom of the page.
- Type in a new password. This goes in the "Password" field, though the password field might say "PSK Password" instead.
- Click Save. This button is at the bottom of the page.
- Click OK when prompted.
- Click System Tools.
- Click Reboot.
- Click OK when prompted.

Password Do's

Z@Rvxq")'n=6

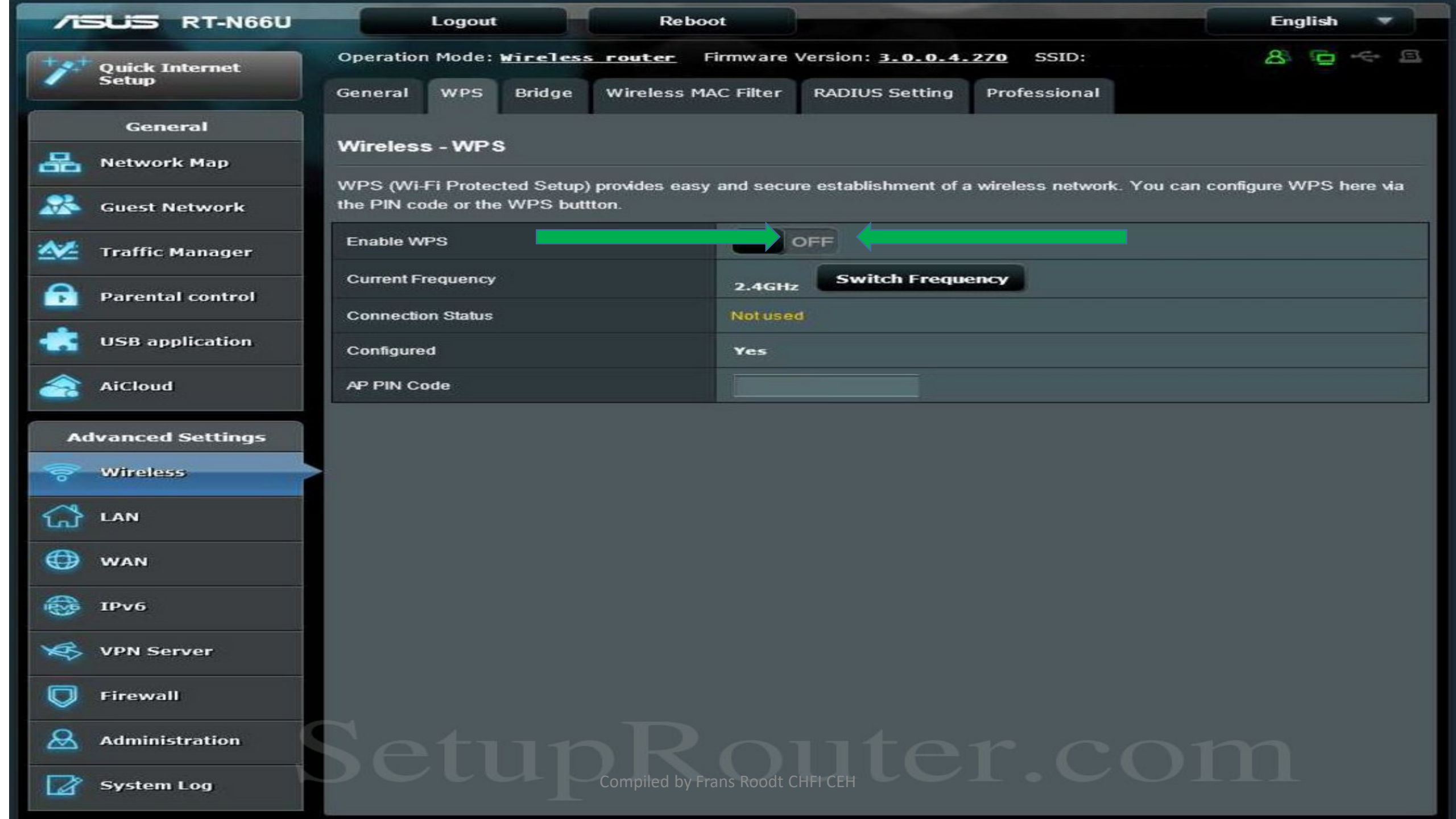
- **Passwords should be long, 8-12-24 a sentence more.**
- **Passwords should be something easy for you to remember, but hard for others to guess or lookup.**
- **Passwords should have lots of different character types: upper and lower case letters, numbers, and symbols.**
- **Replacing letters with symbols is a simple way to achieve this: use @ for a, and (for c, as example.**
- **Passwords are personal, most services have a way to create a 'linked' account or share services with trusted friends and family.**
- **Change passwords regularly. Every 90 to 180 days; this helps keep your accounts from being compromised long-term.**
- **If you must write down a password or make note of it, do so only in specially designed programs, or keep and hold the physical copies with the same care and respect you would a social security card or birth certificate. Remember; anyone with your password "is you".**

Password Don'ts

~~hunter2~~ 

- Don't use short passwords; computers can guess them very easily.
- Don't use a common word you can find in a dictionary.
- Don't use information that can be looked up or guessed, such as a birthday, anniversary, or pet's name.
- Don't use the same password for everything. If one password is compromised, all of the same ones are compromised across all your accounts.
- Don't share passwords. People with your password "are you" to a computer system, or a service.
- Don't keep the same password forever. Assume that, at some point, it will be guessed, seen, or otherwise compromised, and it must be changed.
- Don't write down passwords in the open, or save them in non-encrypted files on your computer.

- Given the information provided on Securing WPS encryption can very easily be cracked within your routers settings on an ASUS router the WPS tab there will be an option to either enable or disable WPS by default this is switched off, leave the setting as is.



Cracking WPS

- Hackers don’t use Windows it’s not a preferred OS to do the job. They use several versions of Linux. Linux Kali is a Penetration testing OS with all the necessary tools a security analyst, Penetration tester can use. There is different types of attacks. My personal favourite
- **Evil Twin**
- This is where a duplicate Access point is setup with the same name as the original. The fake access point de-authenticates the router causing the user to log back in. When this happens the attacker has the password.

Social Engineering

The most successful attacks are not achieved through Software tools. Although there is some that's just as successful.

The Social Engineering Toolkit was created by Dave Kennedy the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social Engineering.

Unfortunately the tool can be used for evil purposes as well, social engineering is one of the hardest attacks to defend against as your anti virus program, router firewall won't pick this one up.

There are many types of social engineering attacks its crucial that we can identify these.

Types of Social Engineering Attacks

Social engineering attacks, which Verizon reports were used in 33% of the data breaches in 2018, can occur:

or By using any combination of these and other avenues of attacks

- **Via face-to-face interactions,**
- **Over the phone (vishing, or what's known as voice phishing),**
- **Over SMS text message phishing (smishing), SMS spam messages**
- **Using email phishing tactics (such as phishing)**

You can easily be Hacked Everyone is a Target

The best firewall is a human one, you can have the best firewall pay thousands to protect your organization but if you are properly informed you will be able to identify these and protect yourself. There are plenty of available resources to do this such as Udemy's free online courses, if you feel that's not enough try EC-COUNCILS Secure Somputer user it's expensive but worth it Infosec has a lot of information on Cyber threats aswell

Passwords,Tools

- Lastly lets get back to passwords, there are some password generating tools that can be used if you cannot think of something
- Secure Safe Pro password generator has options between General and advanced that can be selected.
- Strong password generator is another https://strongpasswordgenerator.com/
- These can be used if you are having problems choosing a password

Staying safe online starts with strong passwords. Follow these steps to help keep you, your family, and your friends safe online.

Strong Password Generator

How to make a good strong password

A strong password has:

- at least **15 characters**
- **uppercase letters**
- **lowercase letters**
- **numbers**
- **symbols**, such as ` ! " ? $? % ^ & * ( ) _ − + = { [}] : ; @ ' ~ # | \ < , > . ? /

A strong password is:

- not your **username**
- not your **name**, your **friend's name**, your **family member's name**, or a **common name**
- not your **date of birth**
- not a dictionary **word**
- not like your **previous passwords**
- not a **keyboard pattern**, such as qwerty, asdfghjkl, or 12345678

Password Generator

nZ1xA5gE0sZ9cO0vM3bR

click to copy

Password Length

4 — 32

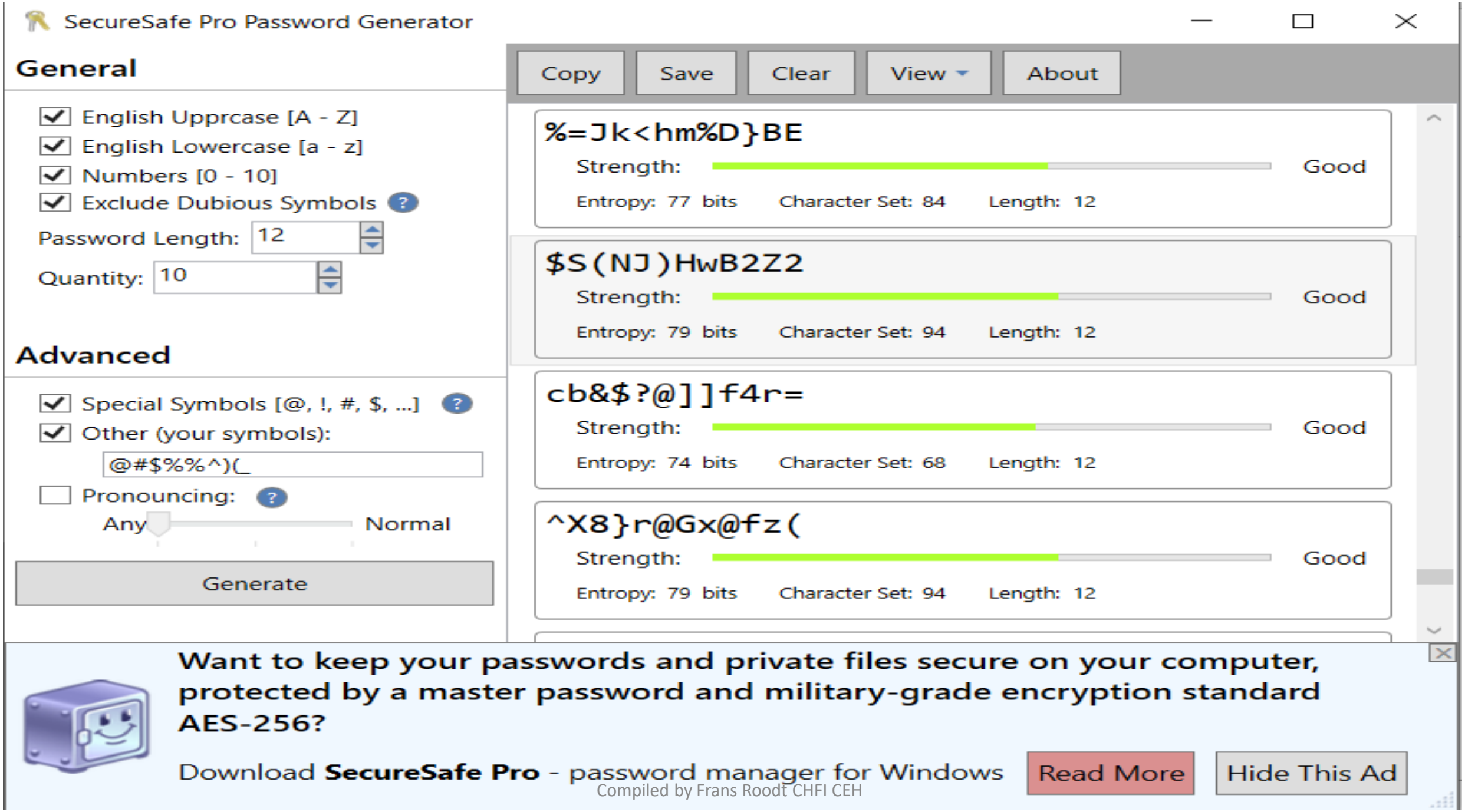
20

Include Uppercase

Include Lowercase

Include Numbers

Include Symbols


SecureSafe Pro Password Generator
General
English Upprcase [A - Z]
English Lowercase [a - z]
Numbers [0 - 10]
Exclude Dubious Symbols
Password Length: 12
Quantity: 10
Advanced
Special Symbols [@, !, #, $, ...]
Other (your symbols):
@#$%%^)(_
Pronouncing:
Any
Normal
Generate
Copy
Save
Clear
View
About
%=Jk<hm%D}BE
Strength: Good
Entropy: 77 bits Character Set: 84 Length: 12
$S(NJ)HwB2Z2
Strength: Good
Entropy: 79 bits Character Set: 94 Length: 12
cb&$?@]]f4r=
Strength: Good
Entropy: 74 bits Character Set: 68 Length: 12
^X8}r@Gx@fz(
Strength: Good
Entropy: 79 bits Character Set: 94 Length: 12
Want to keep your passwords and private files secure on your computer, protected by a master password and military-grade encryption standard AES-256?
Download SecureSafe Pro - password manager for Windows
Read More
Hide This Ad

PASSWORD SALTING

- A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. This is done to defy Brute Force attacks, Dictionary attacks, rainbow table attacks.
- Password salting is part of Cryptography which is a topic way beyond this discussion. A salted password will look like this.
- Password will change to
- **P@|$Wo!d** Which produces a 40 bit hash
- 28720AF614DF1488C20DCB2939723C3528A643F

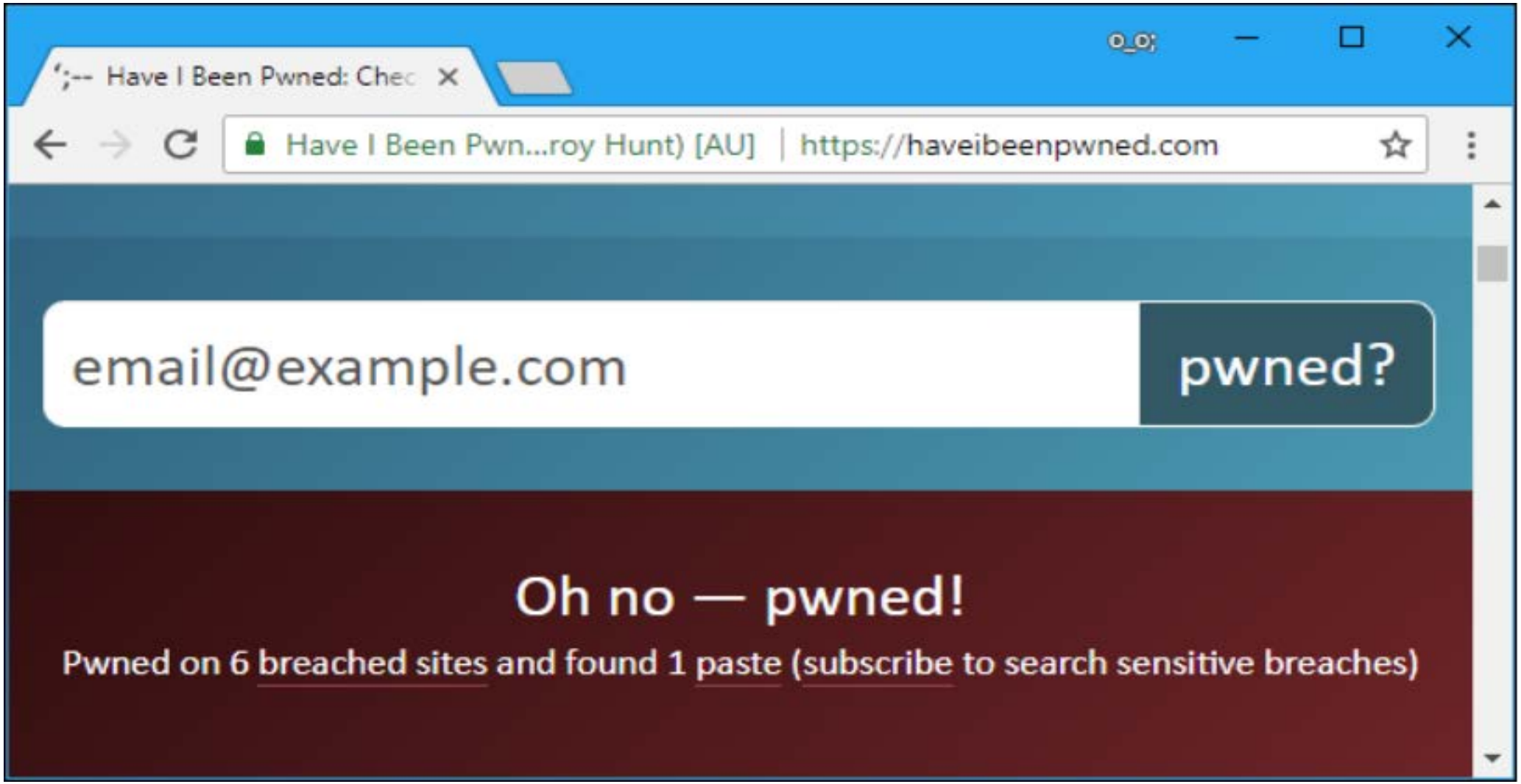
https://haveibeenpwned.com/

- An excellent tool to check if your email address has been compromised in a data breach
- Check if your password has been compromised in a data breach

  How did my account details get stolen?

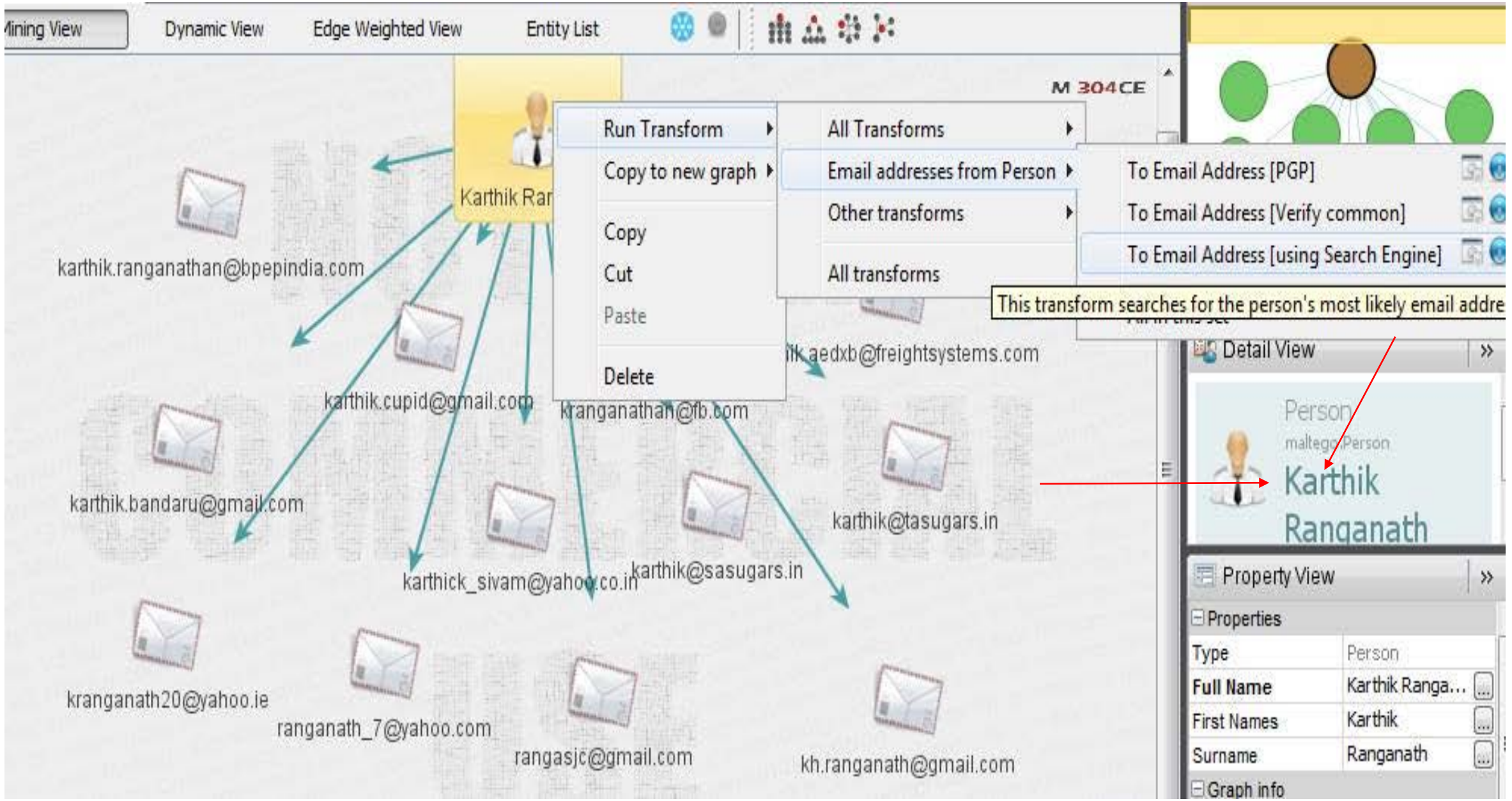
- Every year, billions of login details from hundreds of websites are taken in hacker attacks. These stolen email addresses and passwords are then exposed on the **Dark Web** or sold on the black market, where criminals pay to gain access to your sensitive data. Companies or organizations you do business with can also leak or publish their users' sensitive data by accident.

- If criminals get a hold of one of your accounts, they can potentially impersonate you, message your contacts, access your cloud storage, steal your money, and even jump to your other accounts. That's why we take password safety so seriously.


';-- Have I Been Pwned: Chec
o_O;
Have I Been Pwn...roy Hunt) [AU]
https://haveibeenpwned.com
email@example.com
pwned?
Oh no — pwned!
Pwned on 6 breached sites and found 1 paste (subscribe to search sensitive breaches)

MALTEGO

- Maltego is a social Engineering tool based on Linux. Used by white hat hackers penetration testers and the bad guys this has been included in the Kali Linux Penetration Testing OS. Maintained by Offensive Security. The Tool gathers information on the target each and every internet profile you have registered for. It classifies as an OSINT tool or open source intelligence which means all online information that's publically available. Now we have to come to reality the only way to be safe is not to have internet at all. This however is not possible, the only way to be and stay protected is everything we discussed this far.


Mining View
Dynamic View
Edge Weighted View
Entity List
M 304CE
Karthik Ran
Run Transform
Copy to new graph
Copy
Cut
Paste
Delete
All Transforms
Email addresses from Person
Other transforms
All transforms
To Email Address [PGP]
To Email Address [Verify common]
To Email Address [using Search Engine]
This transform searches for the person's most likely email addre
karthik.ranganathan@bpepindia.com
karthik.cupid@gmail.com
kranganathan@fb.com
ik.aedxb@freightsystems.com
karthik.bandaru@gmail.com
karthik@tasugars.in
karthick_sivam@yahoo.co.in
karthik@sasugars.in
kranganath20@yahoo.ie
ranganath_7@yahoo.com
rangasjc@gmail.com
kh.ranganath@gmail.com
Detail View
Person
maltego.Person
Karthik Ranganath
Property View
Properties
Type
Person
Full Name
Karthik Ranga...
First Names
Karthik
Surname
Ranganath
Graph info

THE HARVESTER

- https://tools.kali.org/information-gathering/theharvester

- The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines

```
*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 3.0.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all

       -s: start in result number X (default: 0)
       -v: verify host name via dns resolution and search for virtual hosts
       -f: save the results into an HTML and XML file (both)
       -n: perform a DNS reverse query on all ranges discovered
       -c: perform a DNS brute force for the domain name
       -t: perform a DNS TLD expansion discovery
       -e: use this DNS server
       -p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
       -l: limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```

WPA-WPA2 CRACKER

https://us.norton.com/internetsecurity-emerging-threats-what-to-do-about-krack-vulnerability.html

Security researchers have discovered a major vulnerability in Wi-Fi Protected Access 2 (WPA2). WPA2 is a type of encryption used to secure the vast majority of Wi-Fi networks. A WPA2 network provides unique encryption keys for each wireless client that connects to it.

Think of encryption as a secret code that can only be deciphered if you have the “key,” and a vital technology that helps keep digital data away from intruders and identity thieves.

The vulnerability, dubbed “KRACKs” (Key Reinstallation Attacks), is actually a group of multiple vulnerabilities that when successfully exploited, could allow attackers to intercept and steal data transmitted across a Wi-Fi network. Digital personal information that is transmitted over the Internet or stored on your connected devices — such as your driver’s license number, Social Security number, credit card numbers, and more — could be vulnerable. All of this personal information can be used toward committing identity theft, such as accessing your bank or investment accounts without your knowledge.

In some instances, attackers could also have the ability to manipulate web pages, turning them into fake websites to collect your information or to install malware on your devices.

Should you change your Wi-Fi password?

No. This vulnerability does not affect the password to your router's Wi-Fi network. Regardless of if your Wi-Fi network is password protected, this new vulnerability still puts your data at risk because it affects the devices and the Wi-Fi itself, not your home router, which is what the password protects.

The researchers who discovered this vulnerability state that the attack could be "especially catastrophic" against version 2.4 and above of wpa_supplicant, a Wi-Fi client commonly used on Linux and Android 6.0 and above.
If you are using an Android phone, you will need to go the manufacturer's website to see if there is a new patch available for this vulnerability.

Are hackers already exploiting this vulnerability?

Short answer Yes.

What else can you do to help protect your connected devices while waiting for a software update?

Keep in mind that it may take some time for the manufacturer of your devices to come up with a security patch. In the meantime, there are extra steps you can take to help secure your devices.

We strongly recommend that users install and use a reputable **VPN** on all their mobile devices and computers before connecting to any Wi-Fi network. By using a secure virtual private network **(VPN)** on your **smartphones and computers**, your web traffic will be encrypted and your data will be safe from interception by a hacker. A VPN creates a “secure tunnel” where information sent over a Wi-Fi connection is encrypted, making data sent to and from your device more secure.

Will a VPN stop a Hacker ?

No it will only make it more difficult from accessing your work, home network. With the advent of AI Artificial Intelligence this will help evolve behavioural Machine learning predicting human behaviour. For example a trusted employee that always came to work early left on time is now staying till late afternoon with unusual download/ Upload patterns. Insider threats disgruntled employees. Defies a firewall / VPN as an employee already know the inner workings of a system.

Nothing is un hackable you can have the most expensive firewall, the most expensive VPN that is not enough. The best protection is the cheapest a Human Firewall if you are aware of the threats you are protected. Without a human element there is no limits into what a hacker can achieve, it's a constant race against good and bad, good and evil. I'll leave you with a final thought. There are different types of hackers and not all are bad. Most of you already know this.

White Hats Good Guys: Penetration testers, System Analysts, Information security officers.

Gray Hats: Choses sides when it suits him.

Black Hats: Bad guys Cyber terrorists

Script Kiddies: Hackers with limited knowledge but can cause similar damage as they are using the same tools while experimenting.

White Hats Good Guys: Penetration testers, System Analysts, Information security officers.
State Nation sponsored hackers

Gray Hats: Choses sides when it suits him. Whistle-blower

Black Hats: Bad guys the usual profile you think of

Cyber Terrorists: Attacking government systems, government departments, CIA, NASA, Pentagon is examples.

Suicide Hackers: These guys don't care if they get caught or serve jail time.

Hacktivists: Hacking groups like Anonymous falls into this category.

Blue Hat Hacker: Revenge simple attacks

Social Media Hacker: is the one who steals social media accounts. This can be done for revenge or gain any information about someone.

Thank You for attending