

CYBER SECURITY AWARENESS SEMINAR



Who am I

- Harjeet Singh Baidwan
- Ethical Hacker, Trainer, Speaker and Consultant.
- Offensive Security Certified Professional (OSCP)
- Found bugs in multiple online sites, online stores and e-commerce websites.

Digitalization

- India ranks 3rd in terms of number of internet users.
- 60 crores people are using internet today.
- It Estimates to 73 crores by 2020
75% new users are from rural area

Why need Cyber Security

- India has been the second most country affected by cyber attacks.
- One in every three internet users faced cyber-attacks.
- 1,852 Cyber attacks hit India every minute.
- 90 per cent's employees and/or leadership personnel lacked cybersecurity awareness and education.

Today's Cyber Security Agenda

- ATM Cloning.
- Online SCAMS.
- Phishing.
- HTTP vs. HTTPS
- Data Sniffing.
- Securing Online Accounts

ATM Cloning and Frauds

- Total ATM fraud cases 980 in 2018-19
- Maharashtra reported 233 cases of ATM fraud in 2018-19, lost Rs 4.8 crore to bank fraud.
- Delhi 179 cases lost Rs 2.9 crore, Tamil Nadu with 147 cases.

ATM Cloning and Frauds



ATM Cloning and Frauds



Online SCAMS

- Fake calls, Email and SMS scams
- Convince you to share your details or click on a link.
- Lottery, Prizes or cash cards.
- Asks to reply to the number with OTP, CVV or ATM pin.
- Call as a Bank employee, Insurance, RBI, Police verification, so on.
- Never gave your OTP, CVV, ATM pin, Aadhar number, phone number to any one.
- **Nothing is Free.**

KBC SCAM



KAUN BANEGA CROREPATI

ALL India Cash Credit Competition Lucky Draw

OFFER

Congratulations You Have Won The Prize Of 35,00,000
By KBC Department Please Collect Your Prize Urgently By Follow The Company rules And Reugaltion

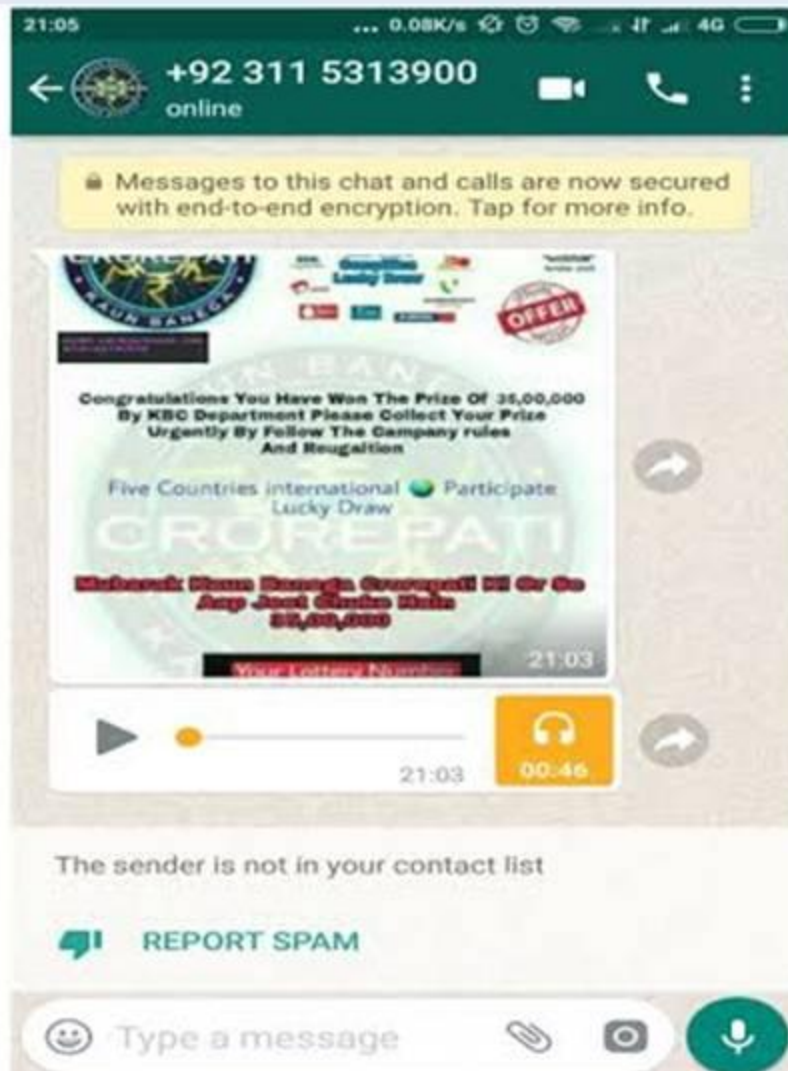
Five Countries international Participate Lucky Draw

Mubarak Kaun Banega Crorepati Ki Or Se Aap Jeet Chuke Hain 35,00,000

Your Lottery Number
89900

ICICI Ban

Mumbai Head Office Numbers
What'sapp Calling **0022588331666**
Mobile Dial **088331666**



21:05 0.08K/s 4G

+92 311 5313900 online

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Congratulations You Have Won The Prize Of 35,00,000
By KBC Department Please Collect Your Prize Urgently By Follow The Company rules And Reugaltion

Five Countries international Participate Lucky Draw

Mubarak Kaun Banega Crorepati Ki Or Se Aap Jeet Chuke Hain 35,00,000

21:03

21:03 00:46

The sender is not in your contact list

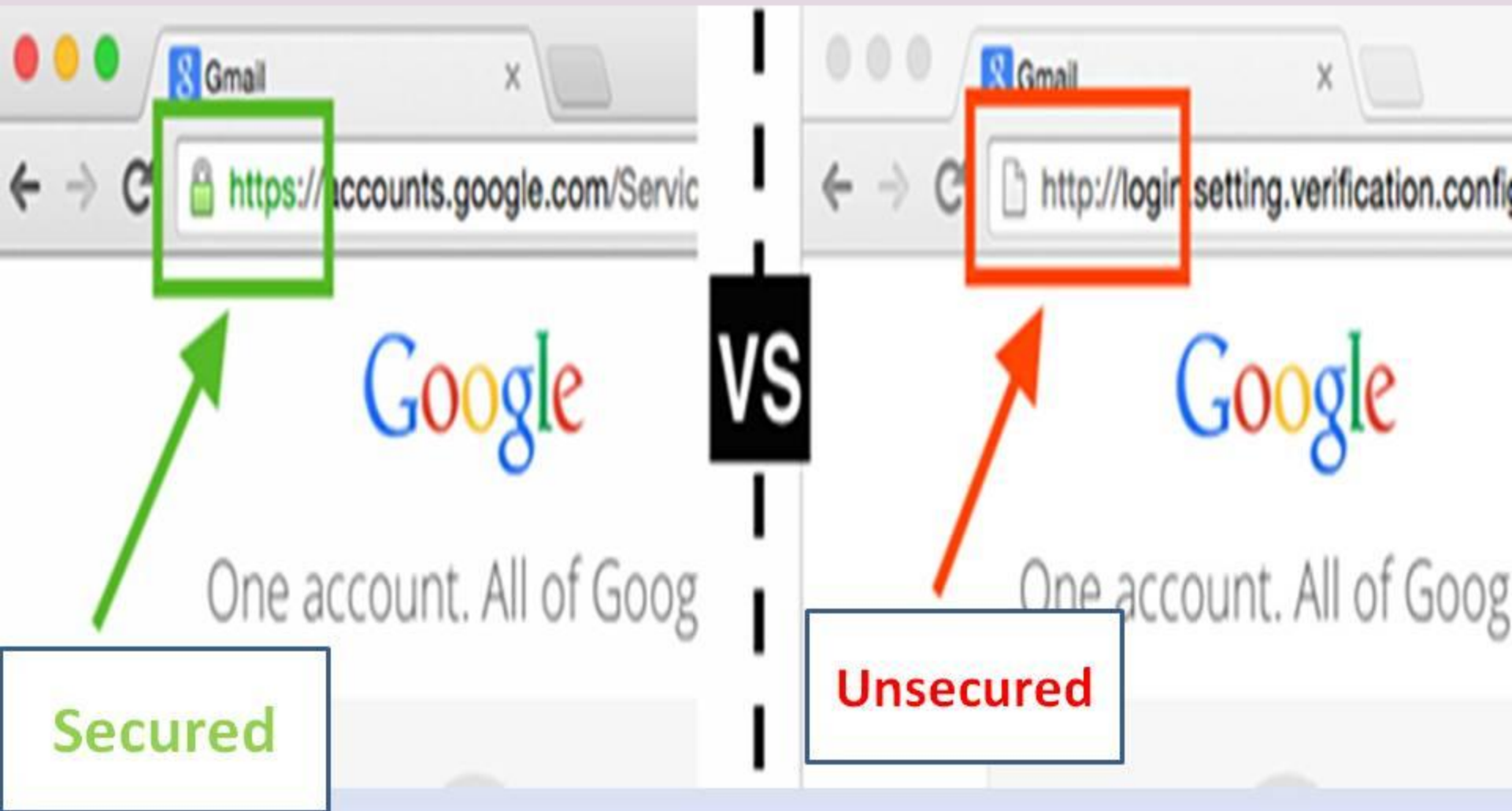
REPORT SPAM

Type a message

HTTP vs HTTPS

- <http://www.google.com>
- HTTP Hyper Text Transfer Protocol
- HTTPS is Secured Hyper Text Transfer Protocol
- Encryption is done between browser and Web server.
- Data sniffing is not possible in https.
- Always use https for transactions, logins, online payments.

HTTP vs HTTPS



Phishing

- Phishing is the way to obtain sensitive information like username, password and credit/debit card details by disguising oneself as a legitimate website in an electronic communication.
- Attacker can send you look alike links on social media sites, WhatsApp, through SMS or Email.
- Eg: Facebook, Gmail, Twitter, LinkedIn login
- After catching your credentials it will redirects you to original website.

Phishing

← → ↻ Not secure | 192.168.43.1



Apps | pics | sql-i | resources | mysql_real_escape_... | bug ind | soluz | learn sec | offsec | Ann Wigmore-The... | Reverse Shell Cheat... | Linux Services Orga...



Sign in with your Google Account



Victim@gmail.com

.....

Sign in

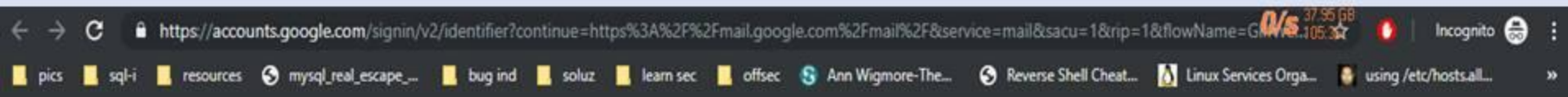
[Need help?](#)


[Create an account](#)

One Google Account for everything Google



Phishing




Sign in
Continue to Gmail

[Forgot email?](#)

Not your computer? Use Guest mode to sign in privately.
[Learn more](#)

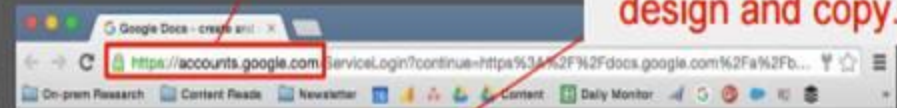
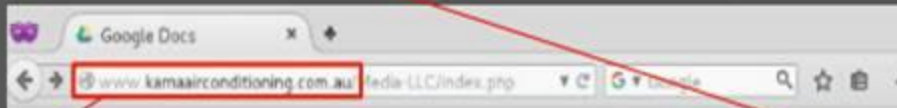
[Create account](#) [Next](#)

Phishing

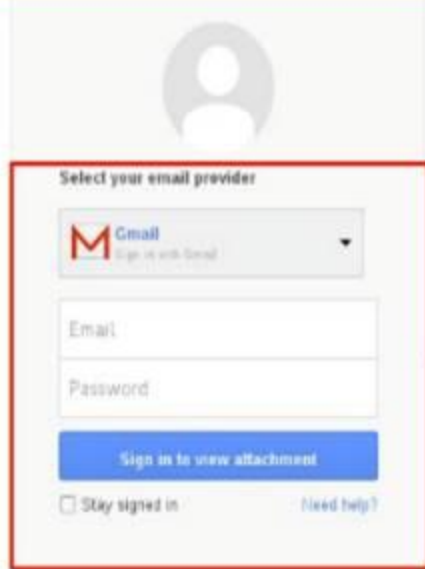
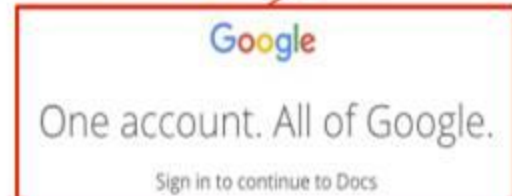
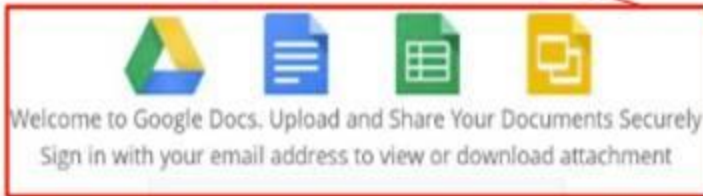
Site has inaccurate design and copy.

Site is directed to a legitimate google.com URL.

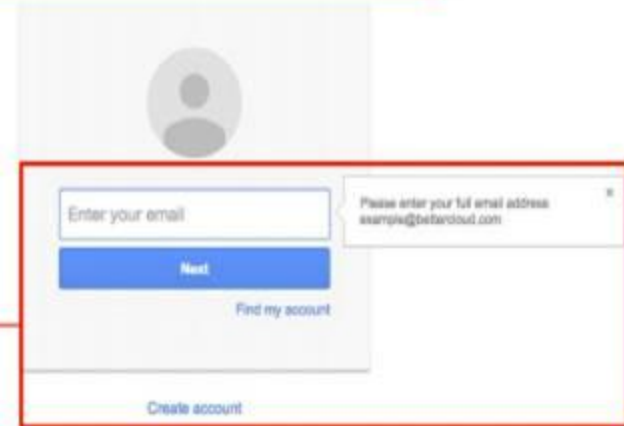
Site has correct design and copy.



Always check the URL when entering your email and password.



Google will never ask you to select your email provider or ask for both email and password on the same screen.



Phishing Quiz

Great job, Harjeet
Singh!
You got 8/8 correct.

Practice makes perfect and the more you understand what to look for, the safer you are from phishing attacks.

You can also take a few simple steps to protect your online accounts better. Learn more at g.co/2SV.

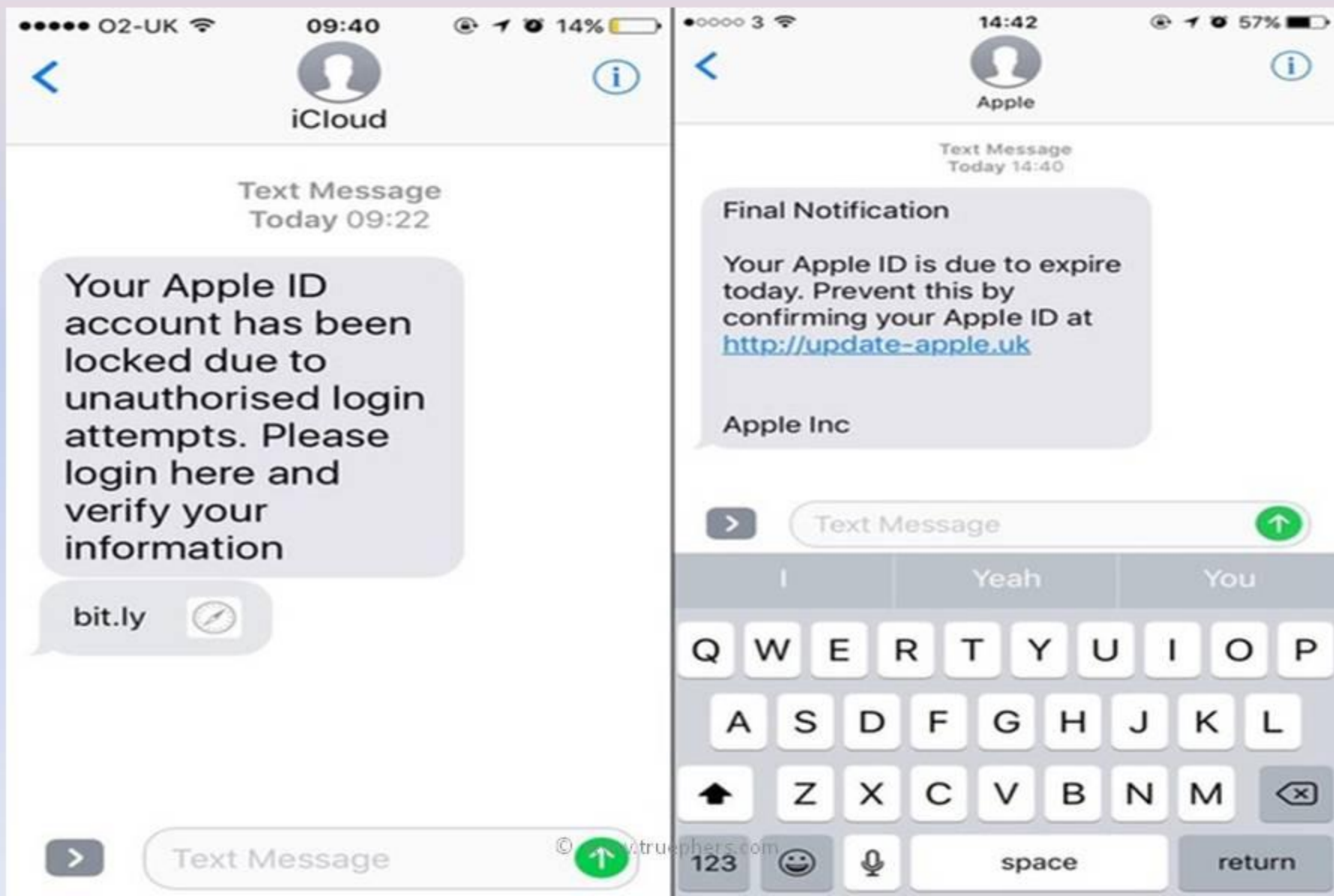
Share the quiz:



TAKE THE QUIZ AGAIN



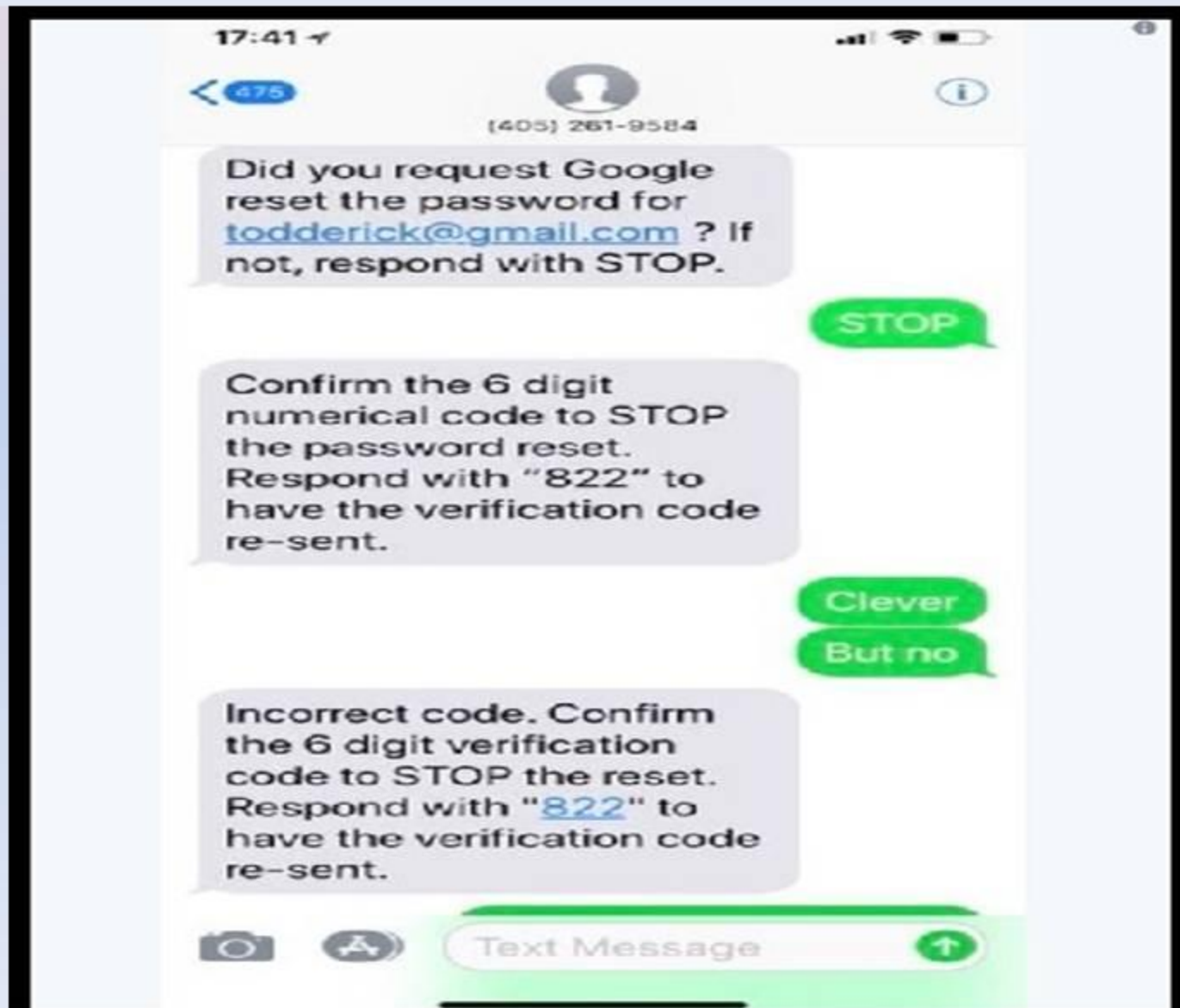
SMiShing



Securing Online Accounts

- Check Facebook Active logins.
- Check Google Active logins.
- Enable 2 Step verification with mobile number.
- Don't use too easy password, that can be guessed.
- Don't share your email id and phone number unnecessarily.

Social Engineering



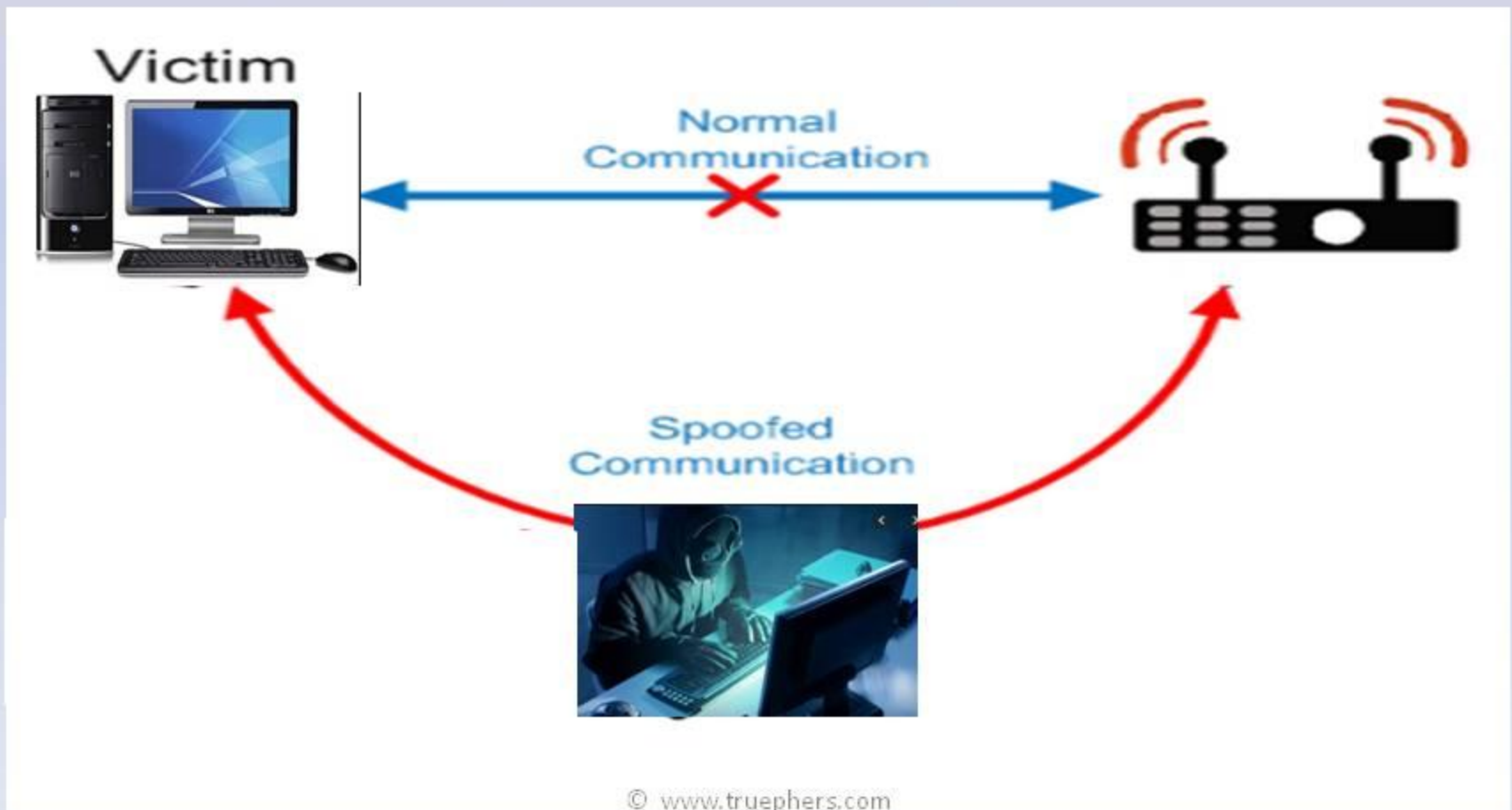
Free Public Wi-Fi

- Free Google station Wi-Fi
- Free City Wi-Fi
- Coffee House
- Restaurants, Hotels
- Schools, Colleges, Offices, Palaces etc.



Data Sniffing

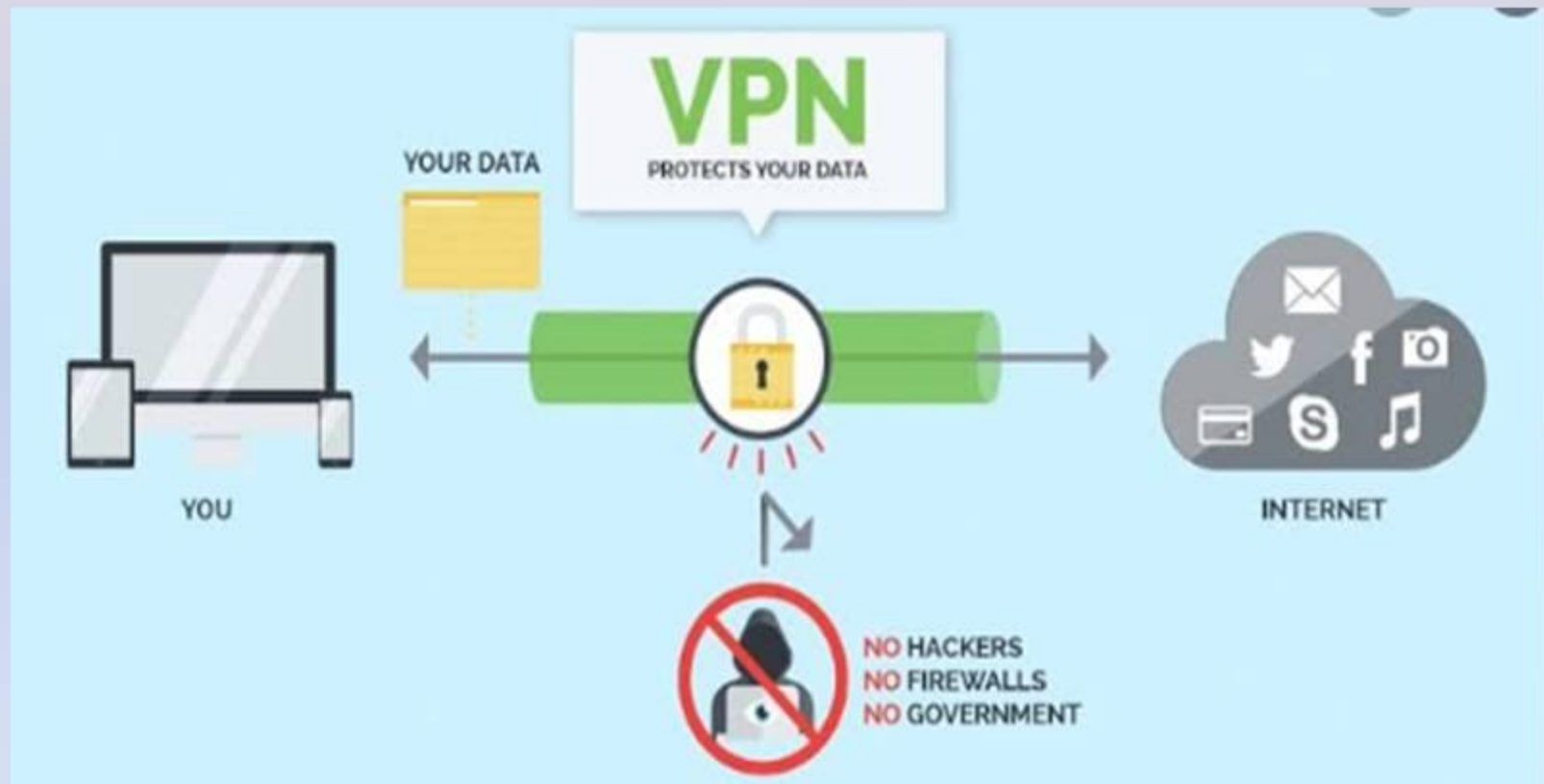
- Sniffing is a process of capturing or monitoring all data packets passing through the network.



Mitigating Data Sniffing

- Active sniffing through mobile devices.
- Never connect to unsafe free hotspot WiFi's
- Use strong Wi-Fi password at home.
- Mitigation on Android Windows Mac and iPhone
- Use VPN software/App available for all devices.

Virtual Private Network





TRUE PHERS



+91 73 994 994 73



<https://www.truephers.com>



@truephersinfosec



<https://fb.com/truephersinfosec>



@truephers



info@truephers.com