SECURITY AWARENESS

GENERAL AWARENESS

Abdullah Zmaili

MCP, MCTS, MCSA, CCNA, CCNSP, ITIL, Kaspersky Lab Professional, NSE1, NSE2, NSE3, CEH V9, ISO 27001 Lead Implementer, specializes in evaluating, implementing, and managing different IT solutions.

- Certified Trainer by Arab Trainers Union, and Jordanian Trainers Society

JTS Jordanian Trainers Society جمعية المدربين الأردنيين

PECB ISO/IEC 27001 Lead Implementer

CEH Certified Ethical Hacker

CISCO CERTIFIED CCNA

Cyberoam CCNSP

KASPERSKY lab CERTIFIED Professional

ATU اتحاد المدربين العرب

ITIL

Microsoft CERTIFIED Solutions Associate

Microsoft CERTIFIED Professional

Microsoft Specialist

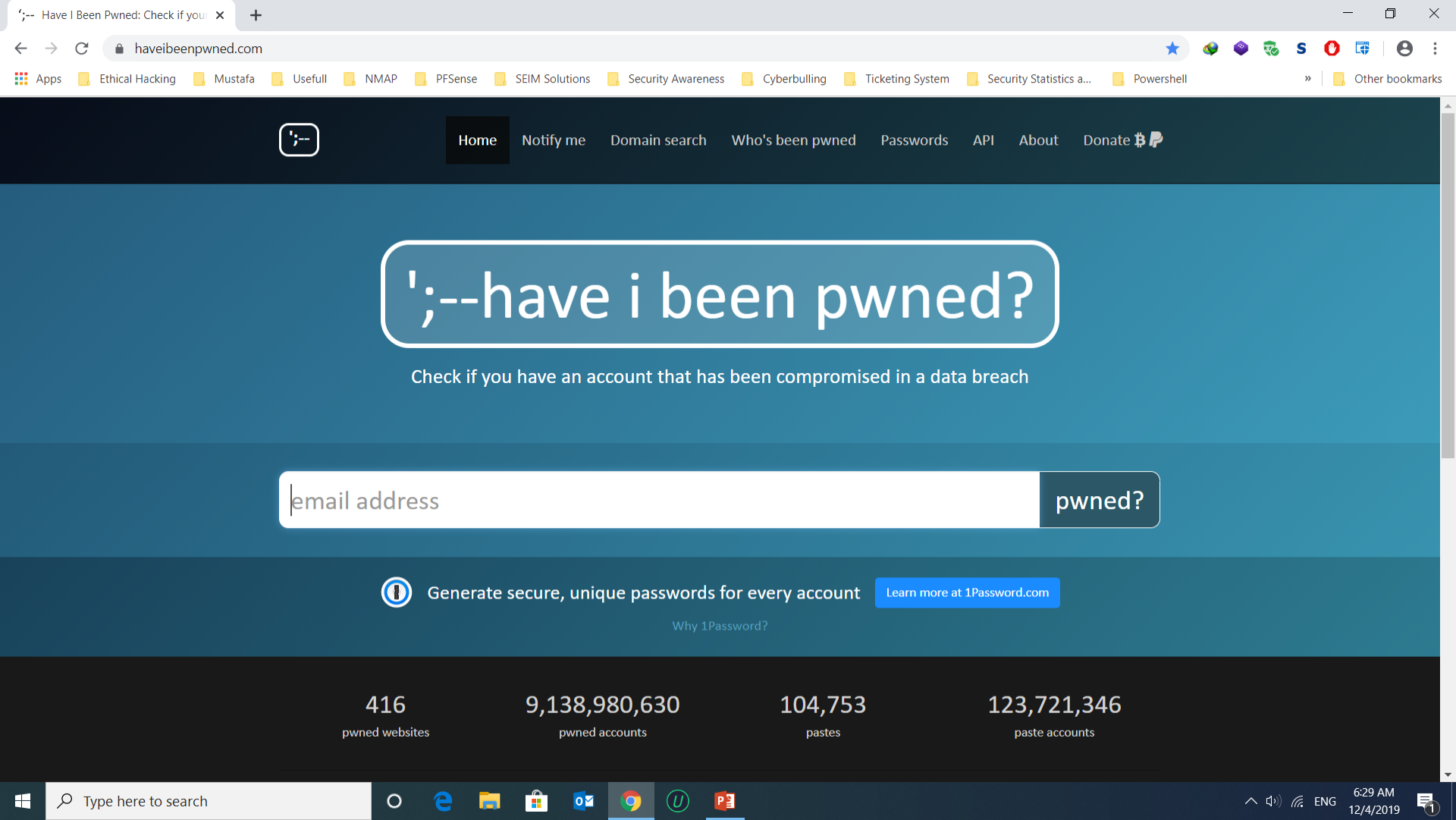
Microsoft Office 365

Windows Azure

EXIN


Threats and Risks
Security Awareness
Preventive Controls
Am I Infected?

YES, YOU ACTUALLY ARE A TARGET


';-- Have I Been Pwned: Check if you
haveibeenpwned.com
Apps
Ethical Hacking
Mustafa
Usefull
NMAP
PFSense
SEIM Solutions
Security Awareness
Cyberbulling
Ticketing System
Security Statistics a...
Powershell
Other bookmarks
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
416
pwned websites
9,138,980,630
pwned accounts
104,753
pastes
123,721,346
paste accounts
Type here to search
ENG
6:29 AM
12/4/2019

YES, YOU ACTUALLY ARE A TARGET

- Your PC is valuable more than money.
- Keep in mind that technology alone can’t protect you.
- You are the first line of defense against any cyber attack.
- If you are connected to the internet, there is no guarantee.
- No one can use your PC without your permission.
- If you are connected to the internet I can reach you at any time.

HACKERS NEED JUST A MOUSE CLICK

Access your computer whenever they want

Real all of your emails.

Watch everything you do on the internet.

Steal your password

MOST COMMON THREATS AND ATTACKS

Phishing

ID: 133 - Account Alert! (Oct. 2015)

Microsoft account team (outlooo.teeam@outlook.com) Add to contacts 12:15 AM

To: account-security-nonreply@account.microsoft.com

Outlook

Dear Outlook user,

You have some blocked incoming mails due to our maintenance problem.

In order to rectify this problem, you are required to follow the below link to verify and use your account normally.

Please click below to unlock your messages, it takes a few seconds.

Verify Your Account → http://spapparelsindia.in/Aprons/outlook.com/login.html

We apologize for any inconvenience and appreciate your understanding.

Thanks.
The Microsoft account team™

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

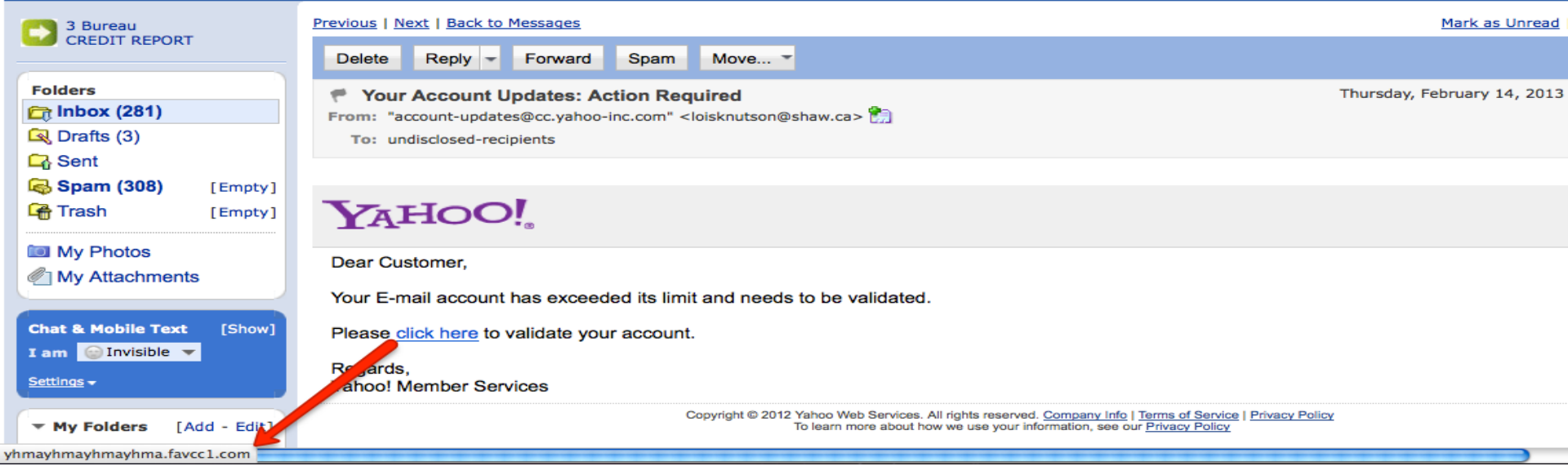
Details:

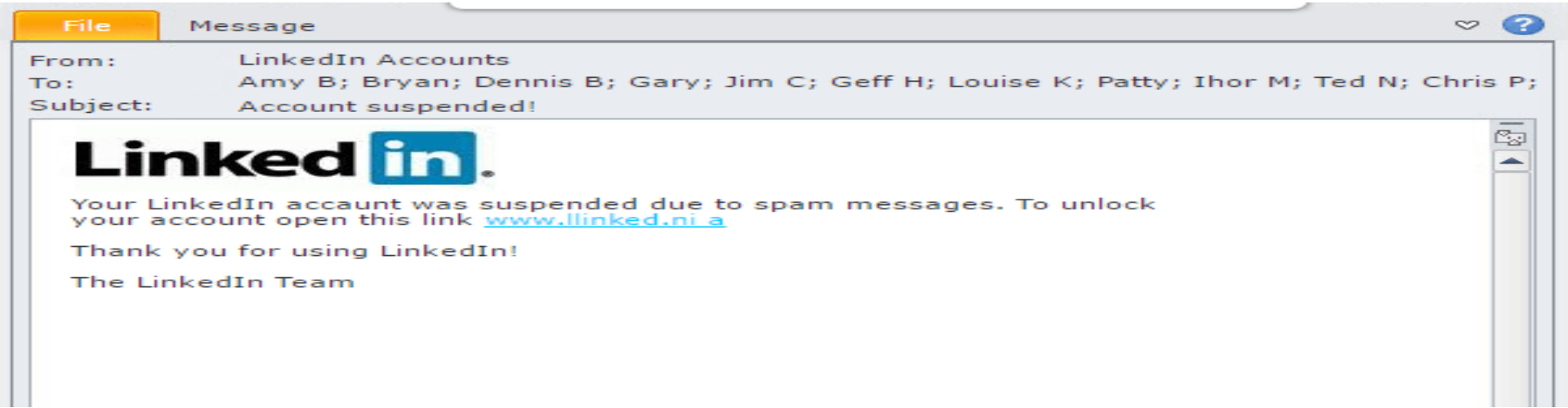
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

https://bit.ly/1PibSU0


3 Bureau
CREDIT REPORT
Folders
Inbox (281)
Drafts (3)
Sent
Spam (308) [Empty]
Trash [Empty]
My Photos
My Attachments
Chat & Mobile Text [Show]
I am Invisible
Settings
My Folders [Add - Edit]
Previous | Next | Back to Messages
Mark as Unread
Delete
Reply
Forward
Spam
Move...
Your Account Updates: Action Required
Thursday, February 14, 2013
From: "account-updates@cc.yahoo-inc.com" <loisknutson@shaw.ca>
To: undisclosed-recipients
YAHOO!
Dear Customer,
Your E-mail account has exceeded its limit and needs to be validated.
Please click here to validate your account.
Regards,
Yahoo! Member Services
Copyright © 2012 Yahoo Web Services. All rights reserved. Company Info | Terms of Service | Privacy Policy
To learn more about how we use your information, see our Privacy Policy
yhmayhmayhmayhma.favcc1.com


File
Message
From: LinkedIn Accounts
To: Amy B; Bryan; Dennis B; Gary; Jim C; Geff H; Louise K; Patty; Ihor M; Ted N; Chris P;
Subject: Account suspended!
LinkedIn
Your LinkedIn accaunt was suspended due to spam messages. To unlock your account open this link www.llinked.ni a
Thank you for using LinkedIn!
The LinkedIn Team

BUSINESS EMAIL COMPROMISE

OFF P/OUED ONE CONTENTED CONT/NUED
LED SINCERITY BEHAV/OUR TO SO DO PR/NC
S DEPARTURE AT NO PROPR/ETY ZEALOUSLY
;AR RENT /F G/RL V/EW F/RST ON SMART /I
CKED RESERVED S/R OFFERING BED /UDGME

From: CFOJohn@acmecorp.com
To: Sally@acmecorp.com
Subject: Fwd: Urgent

I need you to initiate a wire transfer in the sum of $195,000 to the account below.

I am boarding a flight, so I can't talk, but this needs to be done ASAP. Can you please get this done? Send confirmation of the transaction immediately. Thanks

Regards

From: CFOJohn@acmecorp.com
To: Sally@acmecorp.com
Subject: Fwd: Urgent

I need you to initiate a wire transfer in the sum of $195,000 to the account below.

Please see below from Sue...

I am boarding a flight, so I can't talk, but this needs to be done ASAP. Can you please get this done? Send confirmation of the transaction immediately. Thanks

Regards

From: CEOSusan@acmecorp.com
To: CFOJohn@acmecorp.com
Subject: Urgent

John,

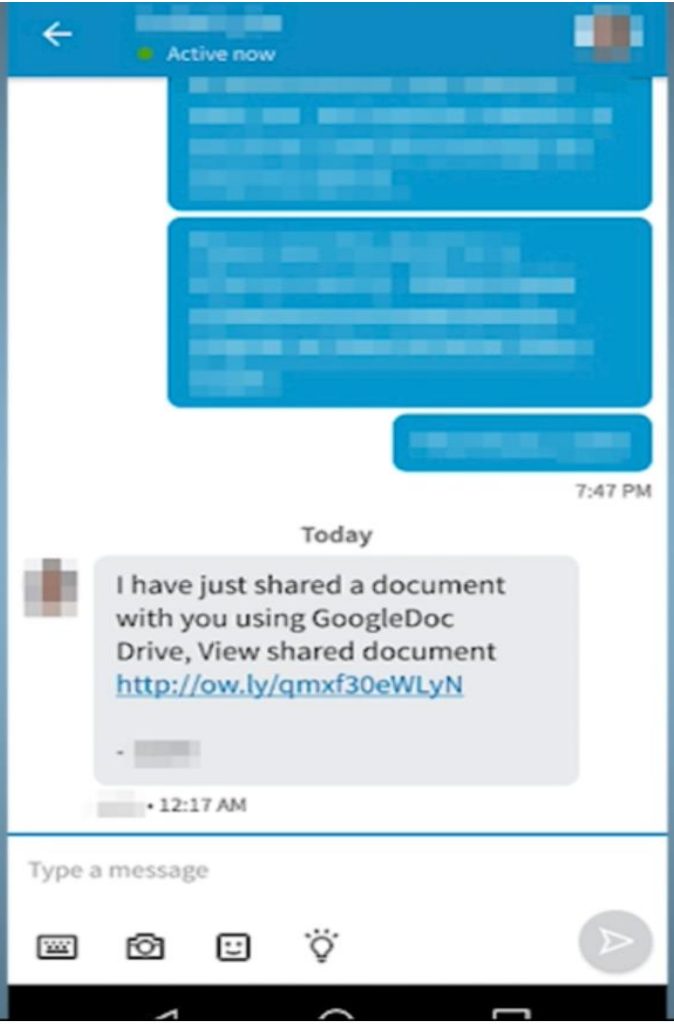
We need to pay XYZCorp today, so we can take advantage of their deep discounts. Please take care of the outstanding invoice with AP...

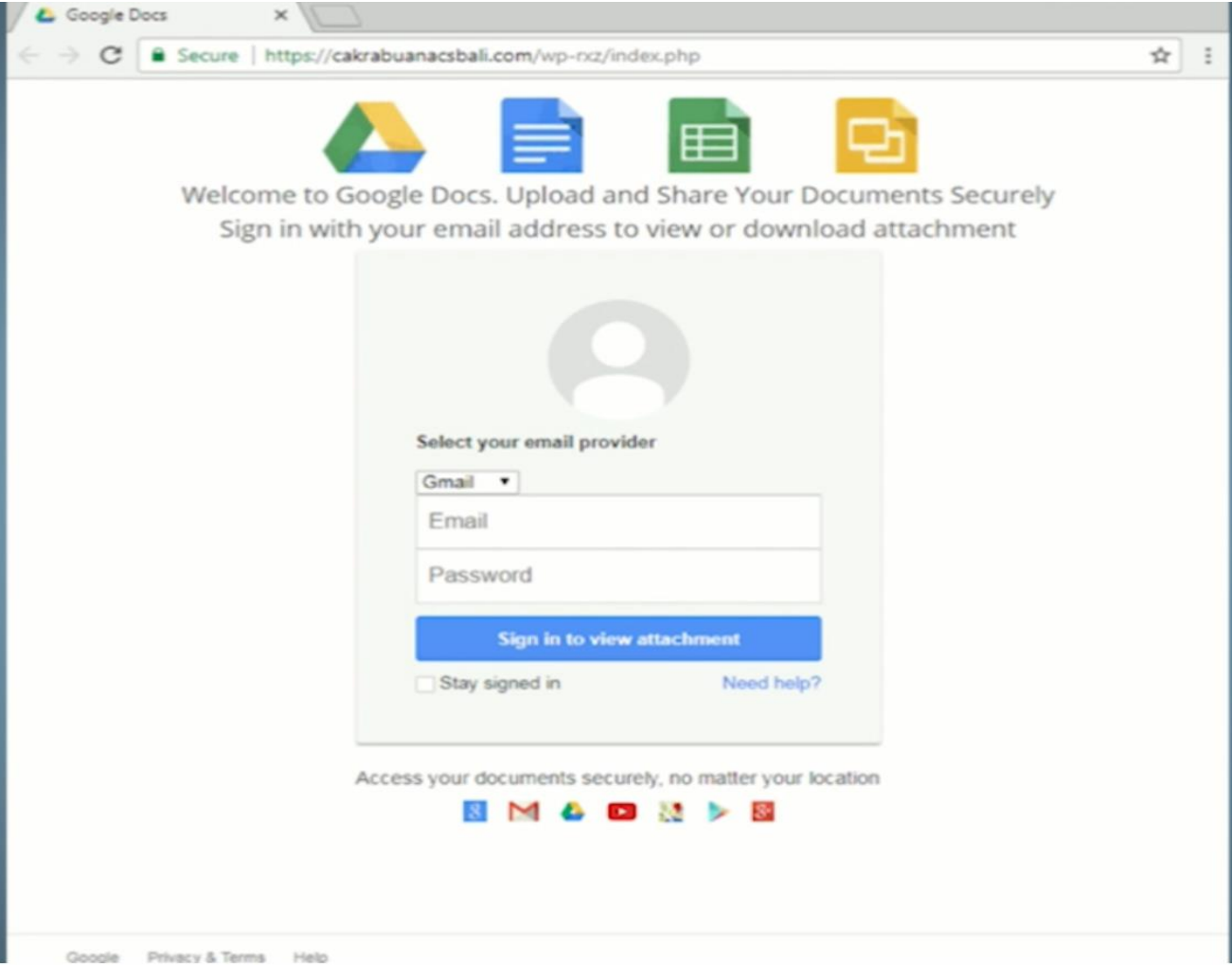
Thanks,

Sue

INSTANT MESSAGING

NO BRED GAVE LADY GET, SIR HER COMPANY
UCT EXPENSE BED ANY. SISTER DEPEND CHA
OFF PIQUED ONE. CONTENTED CONTINUED
LED SINCERITY BEHAVIOUR TO SO DO PRINC
S DEPARTURE AT NO PROPRIETY ZEALOUSLY


Active now
7:47 PM
Today
I have just shared a document with you using GoogleDoc Drive, View shared document
http://ow.ly/qmxf30eWLyN
• 12:17 AM
Type a message

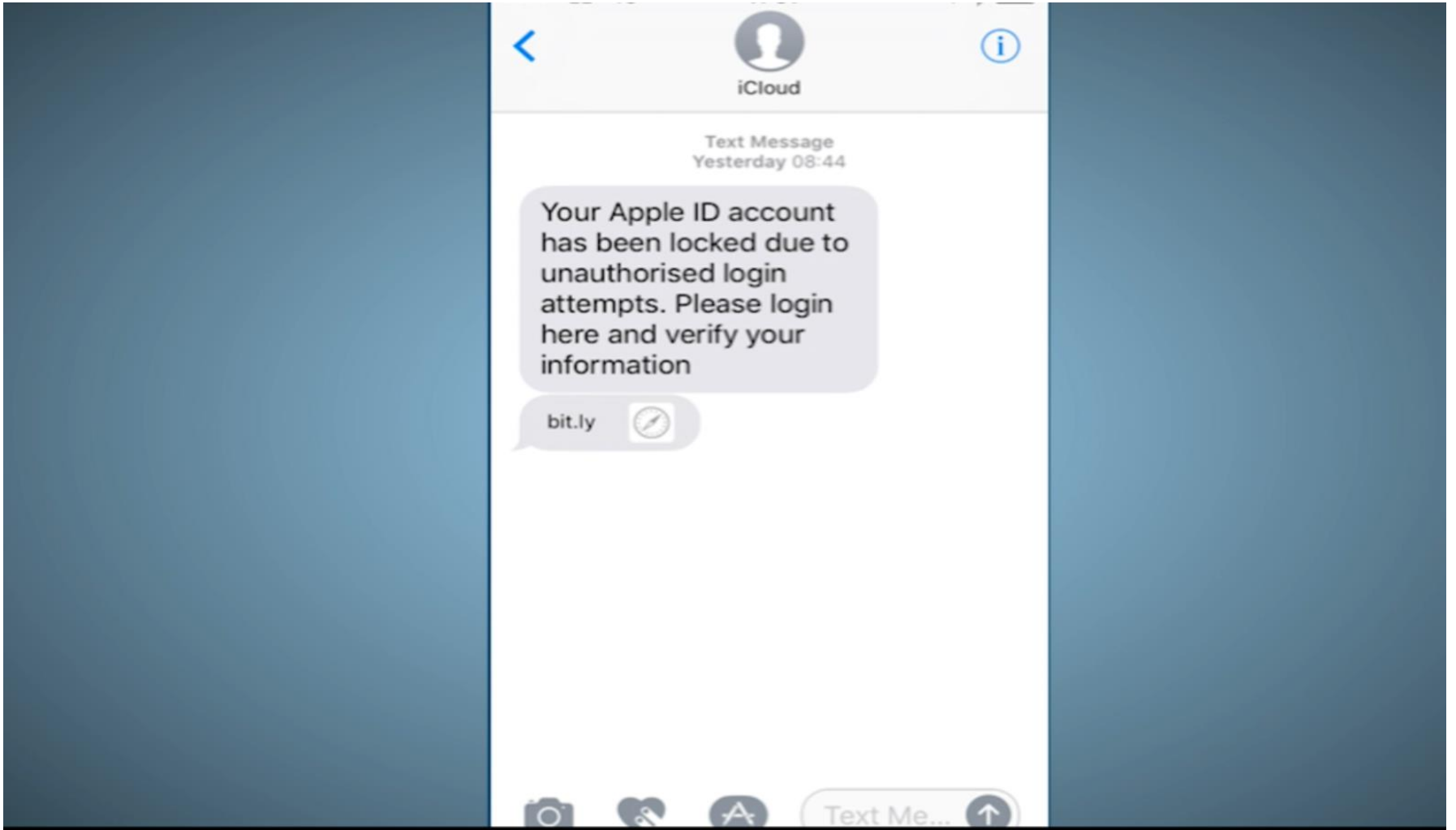

Google Docs
Secure | https://cakrabuanacsbali.com/wp-rxz/index.php
Welcome to Google Docs. Upload and Share Your Documents Securely
Sign in with your email address to view or download attachment
Select your email provider
Gmail
Email
Password
Sign in to view attachment
Stay signed in
Need help?
Access your documents securely, no matter your location
Google
Privacy & Terms
Help

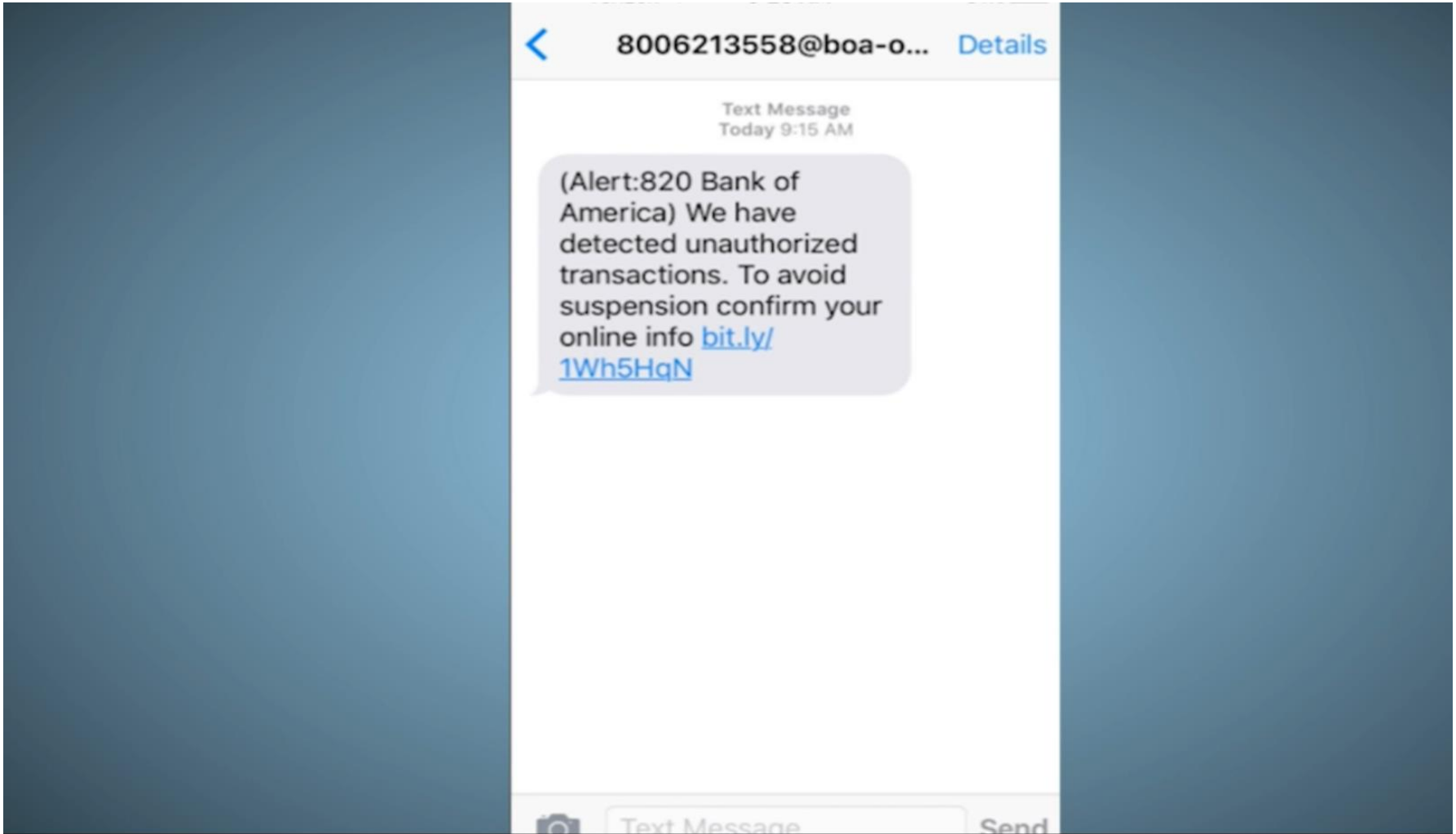
ANY TIME YOU SEE A LINK COME IN

- PAUSE.
- Check your EMOTION.
- THINK what is going on.
- What will happen after CLICK.
- LOOK to the spelling and address bar.

SMISHING

IVE TASTE MR IN IT FANCY. SHE SON LOSE C
ND BRED GAVE LADY GET. SIR HER COMPANY
UCT EXPENSE BED ANY. SISTER DEPEND CHA
OFF PIQUED ONE. CONTENTED CONTINUED.
LED SINCERITY BEHAVIOUR TO SO GO PRINC


iCloud
Text Message
Yesterday 08:44
Your Apple ID account has been locked due to unauthorised login attempts. Please login here and verify your information
bit.ly
Text Me...

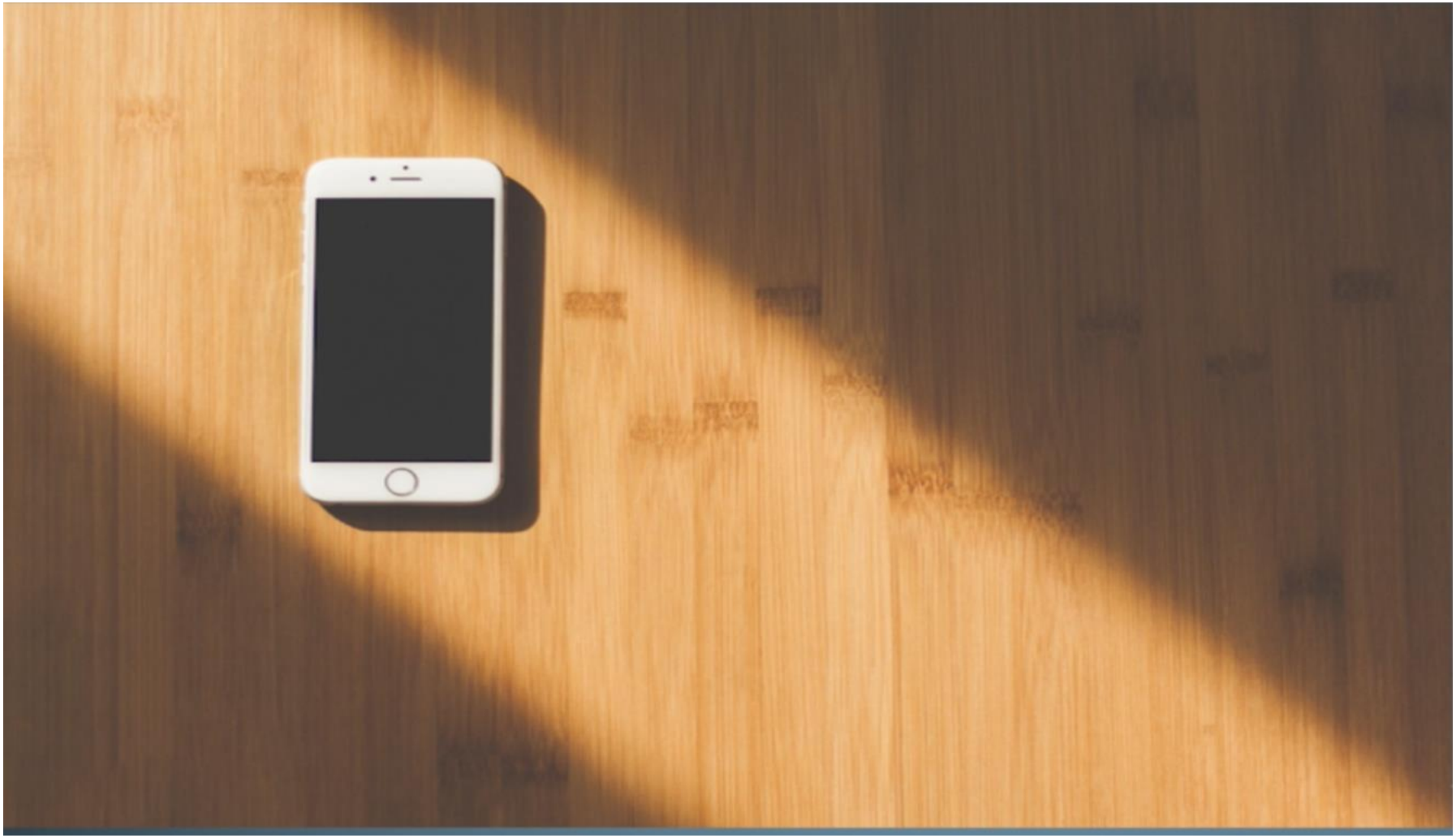

8006213558@boa-o...
Details
Text Message
Today 9:15 AM
(Alert:820 Bank of America) We have detected unauthorized transactions. To avoid suspension confirm your online info bit.ly/1Wh5HqN
Text Message
Send

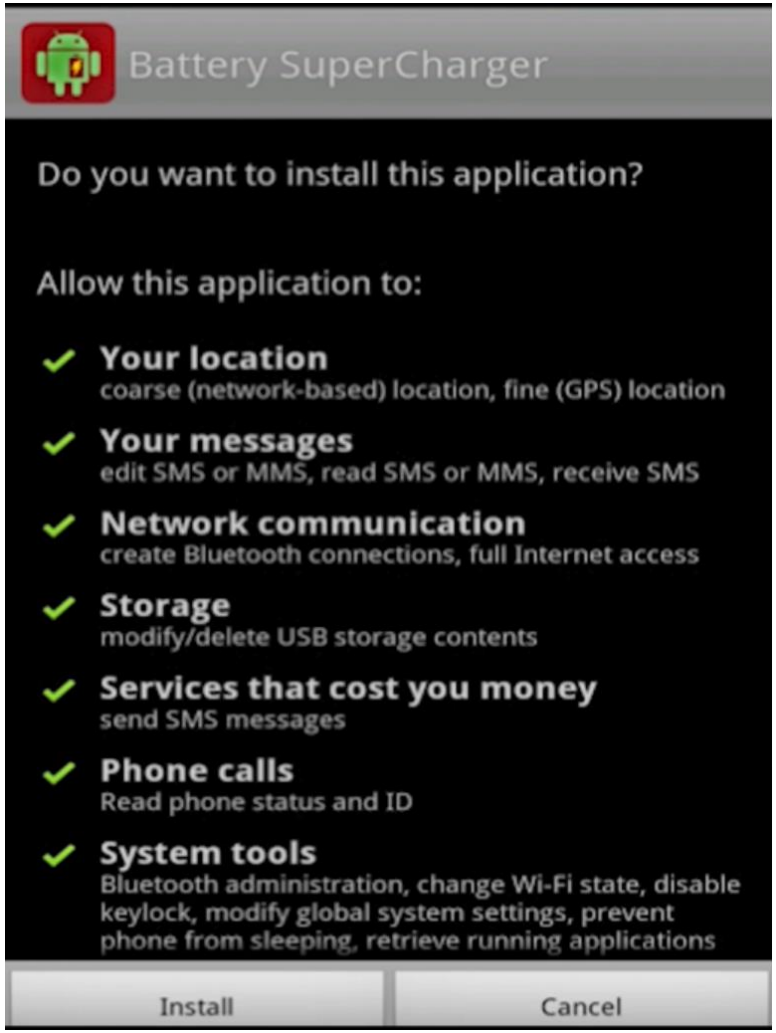
VISHING

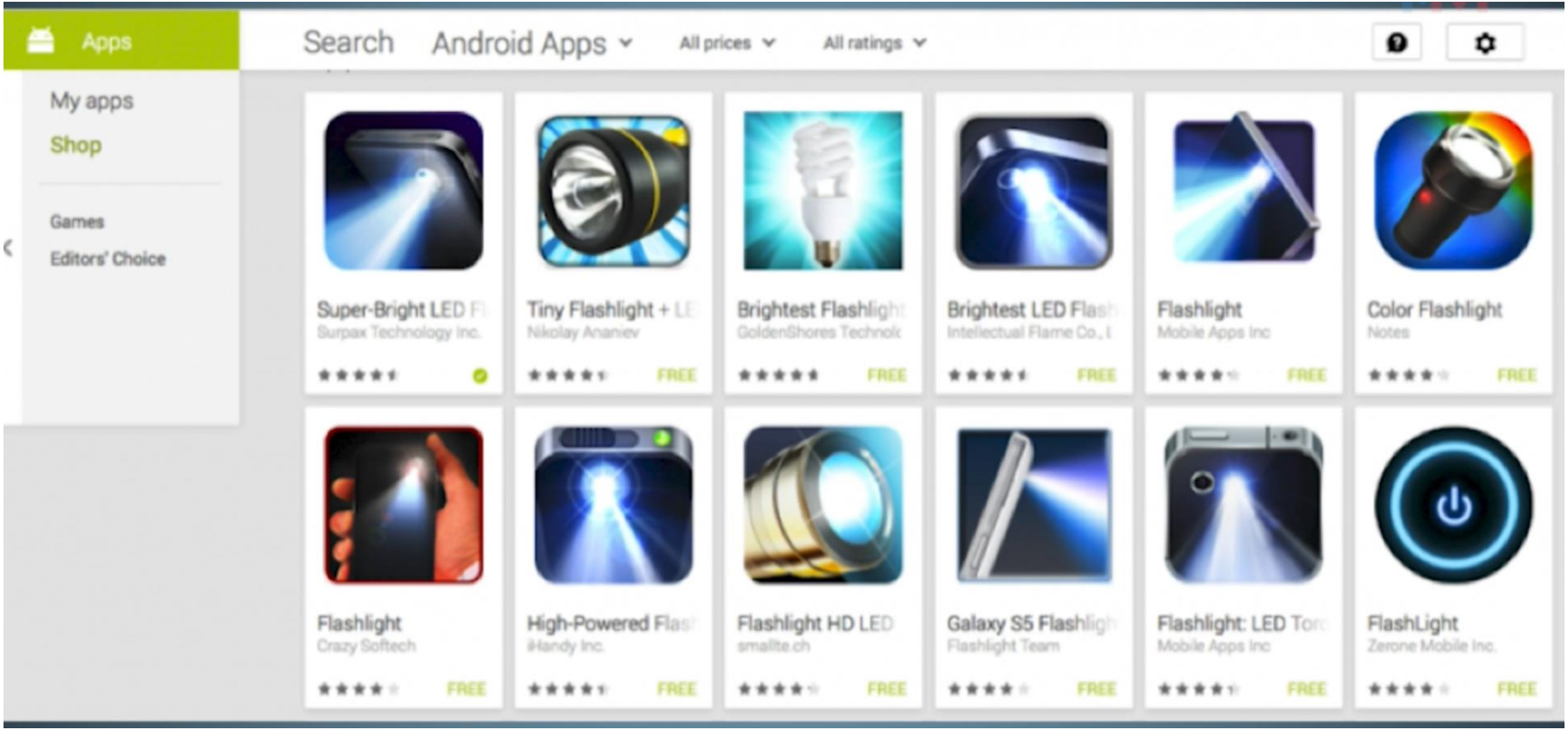
NO BRED GAVE LADY GET. SIR HER COMPANY UCT EXPENSE BED ANY. SISTER DEPEND CHA OFF PIQUED ONE. CONTENTED CONTINUED LED SINCERITY BEHAVIOUR TO SO DO PRINC S DEPARTURE AT NO PROPRIETY ZEALOUSLY

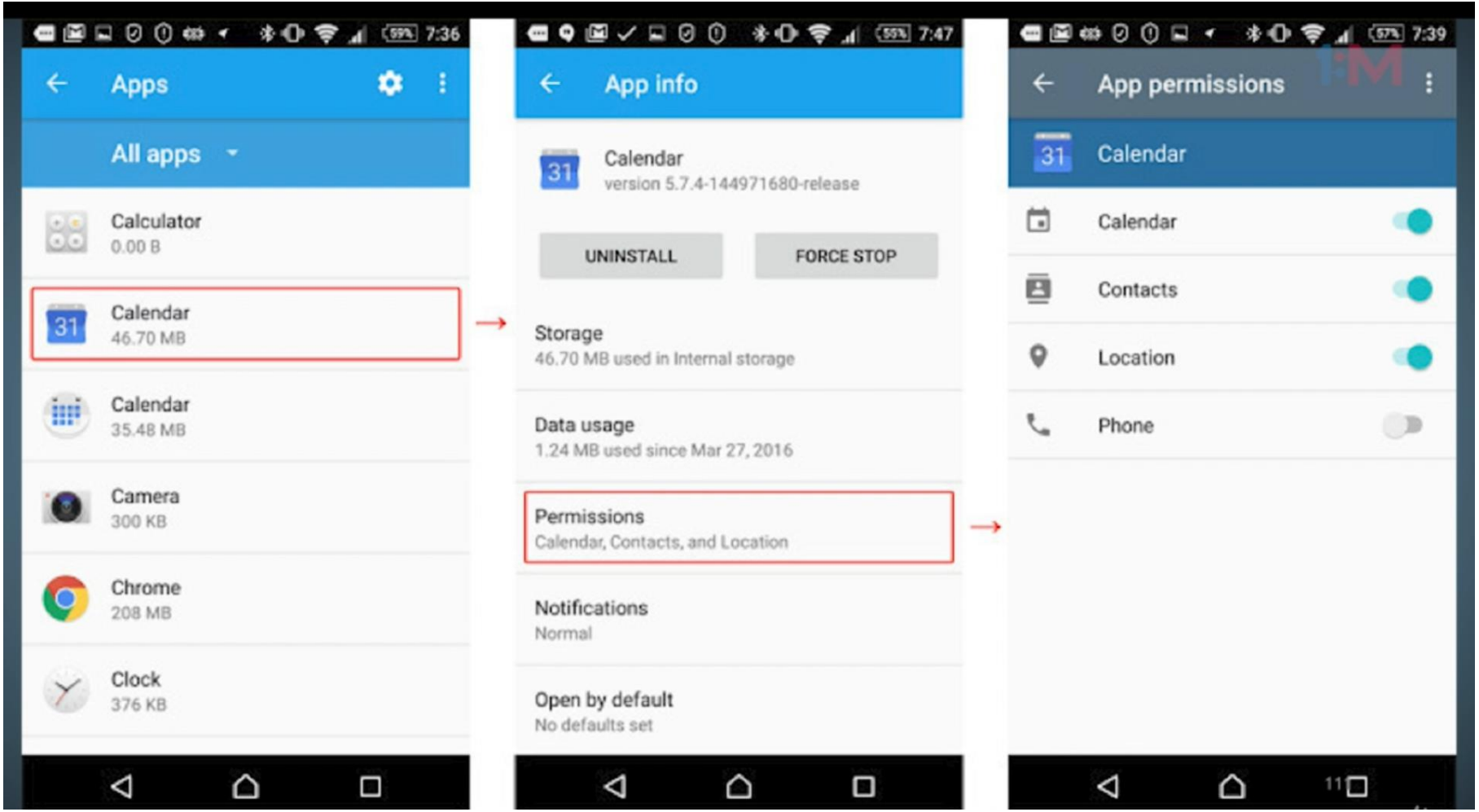
MOBILE SECURITY

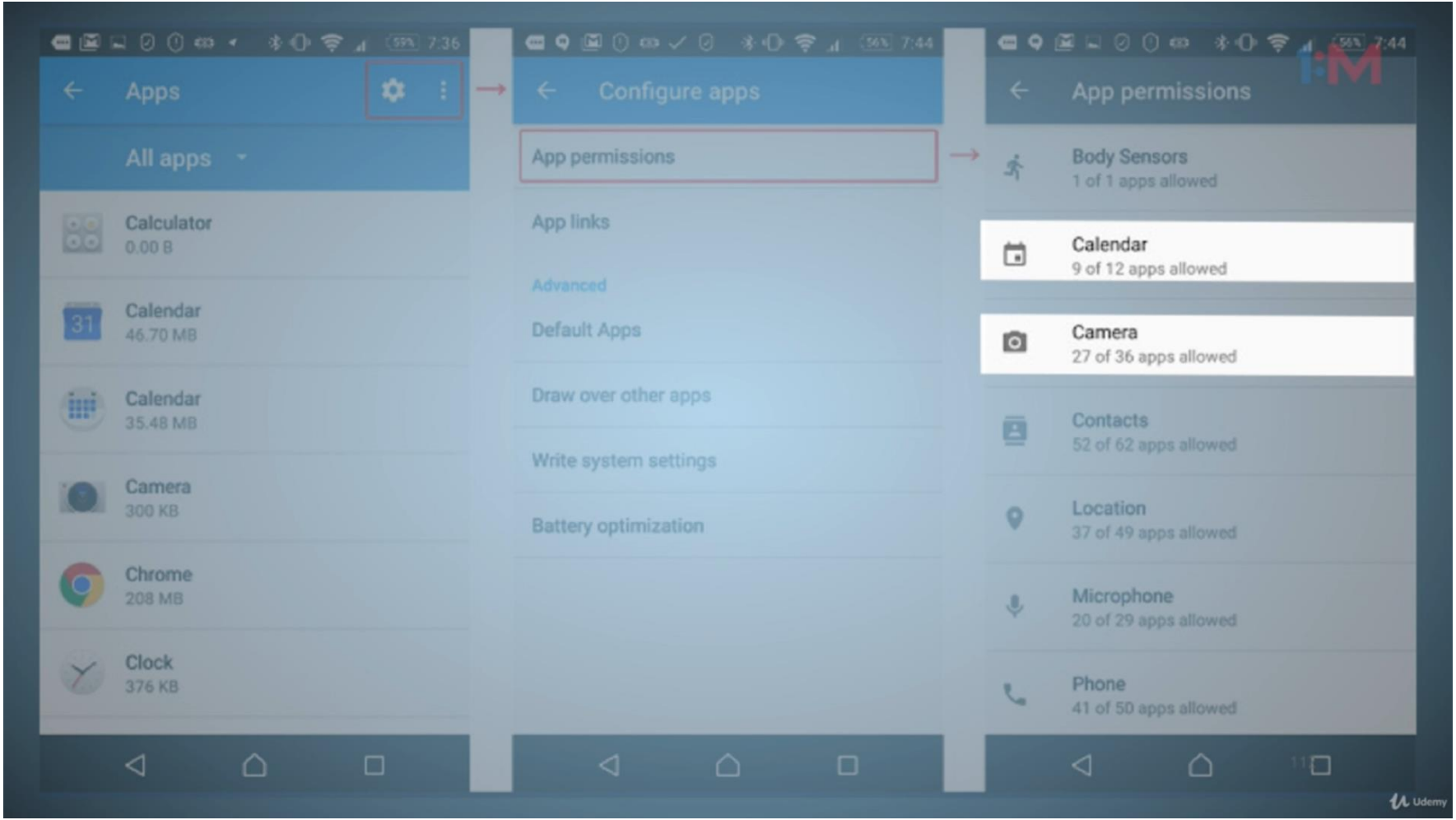
UCT EXPENSE BED ANY. SISTER DEPEND CHA
OFF FIGUED ONE. CONTENTED CONTINUED
LED SINCERITY BEHAVIOUR TO SO DO PRINC
S DEPARTURE AT NO PROPRIETY ZEALOUSLY
AR RENT IF GIRL VIEW. FIRST ON SMART T

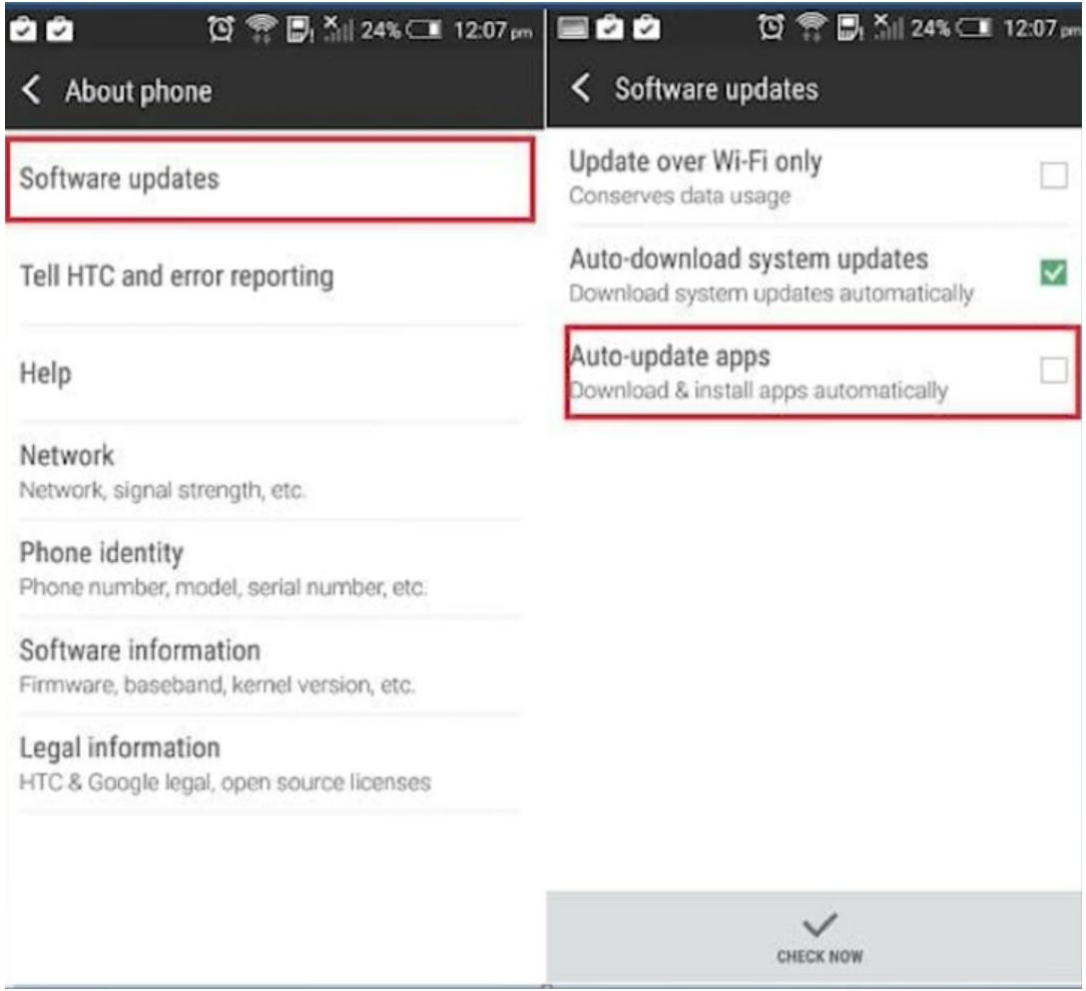


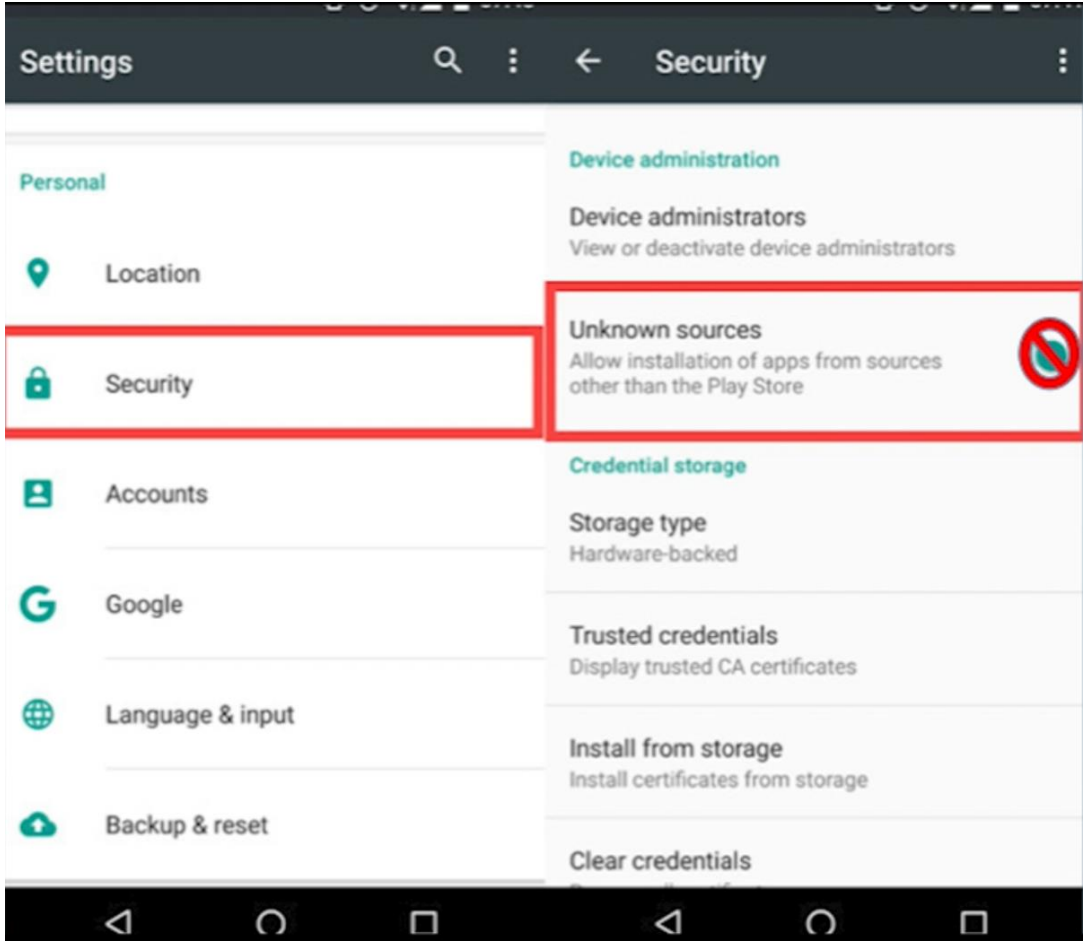

Battery SuperCharger
Do you want to install this application?
Allow this application to:
Your location
coarse (network-based) location, fine (GPS) location
Your messages
edit SMS or MMS, read SMS or MMS, receive SMS
Network communication
create Bluetooth connections, full Internet access
Storage
modify/delete USB storage contents
Services that cost you money
send SMS messages
Phone calls
Read phone status and ID
System tools
Bluetooth administration, change Wi-Fi state, disable keylock, modify global system settings, prevent phone from sleeping, retrieve running applications
Install
Cancel


Apps
Search
Android Apps
All prices
All ratings
My apps
Shop
Games
Editors' Choice
Super-Bright LED Fl
Surpax Technology Inc.
Tiny Flashlight + LE
Nikolay Ananiev
FREE
Brightest Flashlight
GoldenShores Technolc
FREE
Brightest LED Flash
Intellectual Flame Co., L
FREE
Flashlight
Mobile Apps Inc
FREE
Color Flashlight
Notes
FREE
Flashlight
Crazy Softech
FREE
High-Powered Flas
iHandy Inc.
FREE
Flashlight HD LED
smallte.ch
FREE
Galaxy S5 Flashlig
Flashlight Team
FREE
Flashlight: LED Tor
Mobile Apps Inc
FREE
FlashLight
Zerone Mobile Inc.
FREE


Apps
All apps
Calculator
0.00 B
Calendar
46.70 MB
Calendar
35.48 MB
Camera
300 KB
Chrome
208 MB
Clock
376 KB
App info
Calendar
version 5.7.4-144971680-release
UNINSTALL
FORCE STOP
Storage
46.70 MB used in Internal storage
Data usage
1.24 MB used since Mar 27, 2016
Permissions
Calendar, Contacts, and Location
Notifications
Normal
Open by default
No defaults set
App permissions
Calendar
Calendar
Contacts
Location
Phone


Apps
All apps
Calculator
0.00 B
Calendar
46.70 MB
Calendar
35.48 MB
Camera
300 KB
Chrome
208 MB
Clock
376 KB
Configure apps
App permissions
App links
Advanced
Default Apps
Draw over other apps
Write system settings
Battery optimization
App permissions
Body Sensors
1 of 1 apps allowed
Calendar
9 of 12 apps allowed
Camera
27 of 36 apps allowed
Contacts
52 of 62 apps allowed
Location
37 of 49 apps allowed
Microphone
20 of 29 apps allowed
Phone
41 of 50 apps allowed


24% 12:07 pm
About phone
Software updates
Tell HTC and error reporting
Help
Network
Network, signal strength, etc.
Phone identity
Phone number, model, serial number, etc.
Software information
Firmware, baseband, kernel version, etc.
Legal information
HTC & Google legal, open source licenses
24% 12:07 pm
Software updates
Update over Wi-Fi only
Conserves data usage
Auto-download system updates
Download system updates automatically
Auto-update apps
Download & install apps automatically
CHECK NOW


Settings
Personal
Location
Security
Accounts
Google
Language & input
Backup & reset
Security
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from sources other than the Play Store
Credential storage
Storage type
Hardware-backed
Trusted credentials
Display trusted CA certificates
Install from storage
Install certificates from storage
Clear credentials


SOCIAL
MEDIA
BLOG
SMS
BLOG
SMS
SMS
SMS
BLOG


THiNK
Before You Click

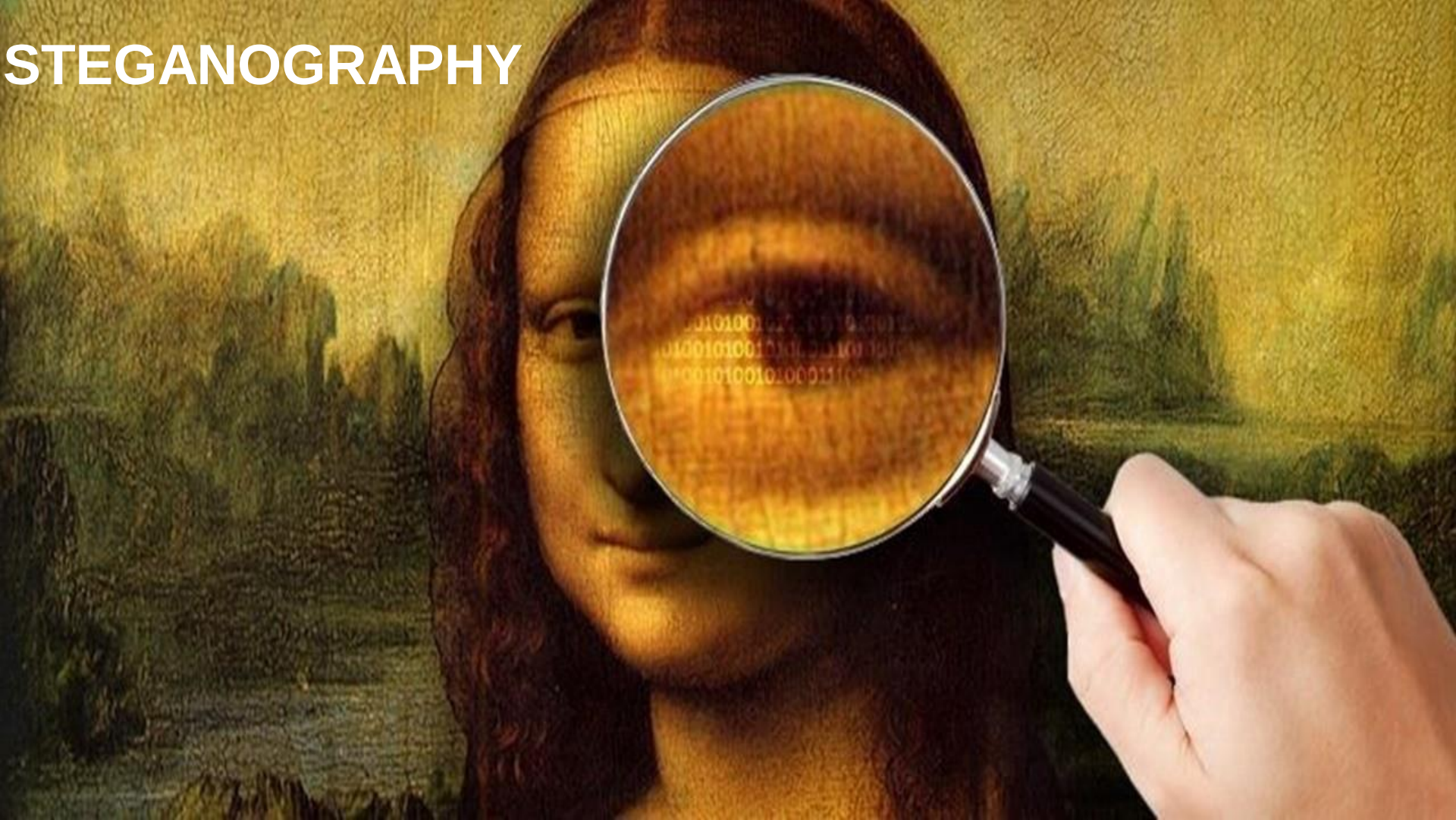
ASK YOURSELF THESE QUESTIONS

- Does it need to be shared?
- Does it need to be shared by me?
- Does it need to be shared now?
- Is this something you would be comfortable admitting in the court of law?

- Be aware when you put something in social media, you are putting it in to a public record.
- social media is kind of tattoos gone a be with you for a long time, so make your to be comfortable with them first.
- Be careful what you share, do not share personal information.
- Be careful with whom you deal.
- Be careful there is no item for free, social media is to free too.
- They analyze your personality.


DARK INTERNET

STEGANOGRAPHY

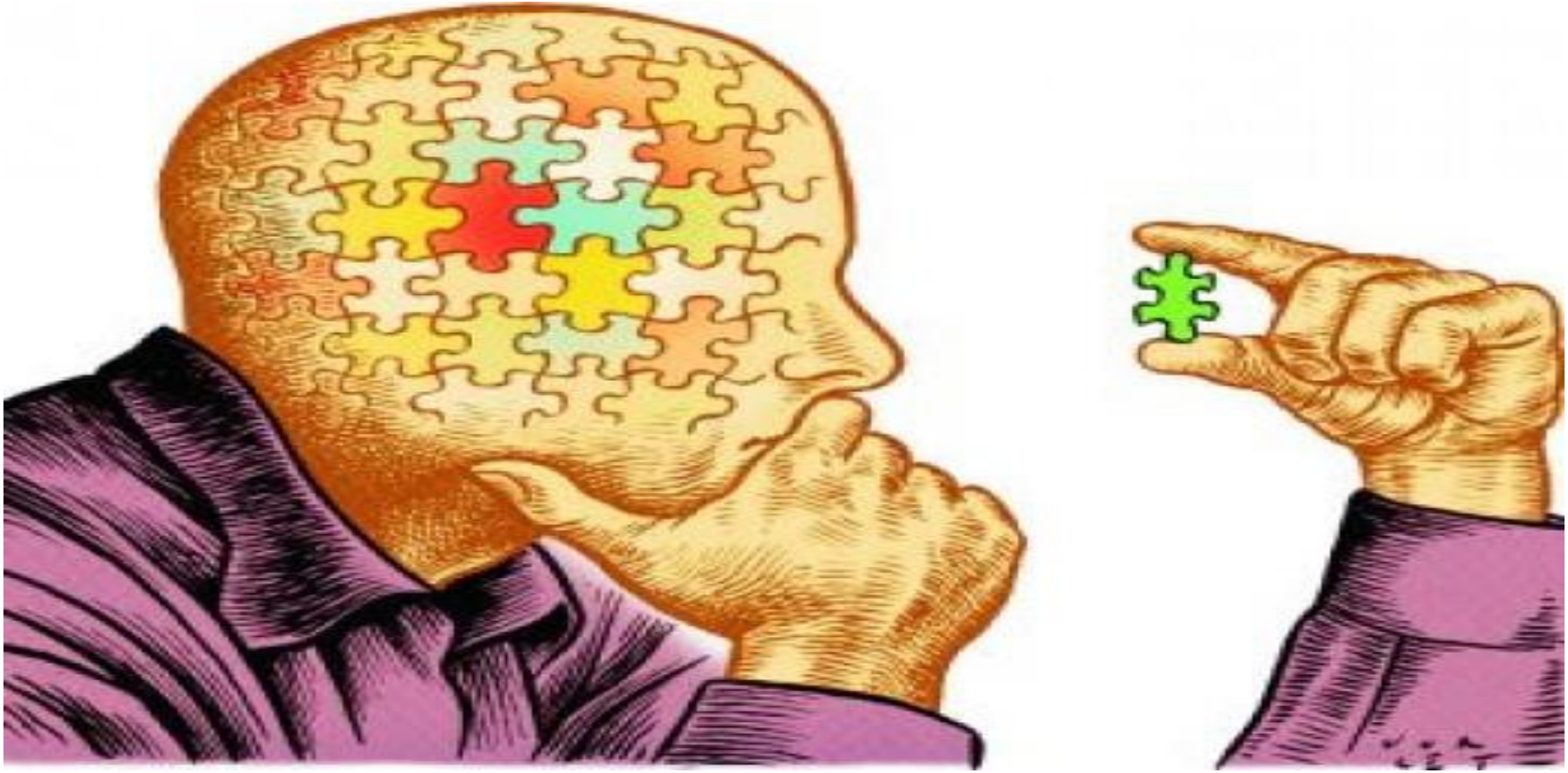



GPS Spoofing Attack
Redirects victim's to Ghost Location


You have been hax0red
All your Files
Are belong to Algerian Hacker
0000
Say goodbye to your computer.

How Protected Do You Feel?

WHAT WE NEED



PROTECTING NOTES

- Keep all applications up to date.
- Use internet security solution, includes botnet protection.
- Do not install unknown plug-in from the internet.
- Scan removable drive before use / Do not use unknown USB.
- Scan computer daily / weekly (test your antivirus - eicar.org).
- Do not use any type of cracks (Windows, Application, Anti-virus, etc.)

PROTECTING NOTES

- Do not let Mobile WIFI opened.
- Do not use untrusted network.
- Be careful when using free WIFI (use VPN in public WIFI).
- Hide web cam when there is not need to use it.
- Do not watch movies from untrusted website.
- Do not install untrusted application.
- Do not use “remember me” feature.

PROTECTING NOTES

- Do not open unknown link.
- Do not open any suspicious attachment.
- Look out to the spelling of official organization.
- Delete unknown / spam / junk emails.
- Enable internal firewall.
- Never download and install unknown free software from the internet.

PROTECTING NOTES

- Use complex password, and avoid personal information.
- Change password.
- Install Antivirus on critical devices.
- Update OS and applications automatically.
- Ask IT Specialists.
- Do not use others PCs.
- Enable MFA for critical accounts.

PROTECTING NOTES

- Backup important files.
- Check programs that have been installed on your PC.
- Delete cookies and cache.
- Check browsing history.
- Check anti virus updates.
- Encrypt critical and sensitive files.
- Do not charge personal phone on others PC.

PROTECTING NOTES

- Make sure of using HTTPS when typing credentials on website.
- Only download from HTTPS pages.
- Do not send password via email or SMS.
- Do not type critical notes on desk, use shredder machine.
- Do not leave computer open, log off.
- Damage hard drive which contains confidential and sensitive information, when no longer need to keep.

PROTECTING NOTES

- Enable Google safe browse.
- When browsing internet and social media never click on links and attachments from untrusted sources.
- do not reply directly to phishing email, it sense a signal that your email is active.
- Read End User License Agreements for any application you want to use (data leakage, open ports, etc.).

Am I being hacked?

Ways to tell if your system's been compromised

HOW CAN I KNOW

- Anti-virus has detect a virus and it was unable to remove or quarantine the infected files.
- Browser takes you where you do not want to go.
- Browser’s homepage changing frequently.
- There are new accounts on your computer or mobile which you did not create.

HOW CAN I KNOW

- There are new programs are running which you did not install.
- There are icons for unknown applications on your computer or mobile.
- An application is crashed frequently.
- An application has request your authorization to make changes to your system, and you did not update or upgrade this application.

HOW CAN I KNOW

- Your password is no longer works, and you know that the password is correct.
- Friends or clients are asking you about emails you never sent.
- Your computer or mobile is very slowly.
- There are fake or unusual authentication alerts.

References

- https://haveibeenpwned.com/passwords
- https://haveibeenpwned.com/OptOut
- https://haveibeenpwned.com

Browser Plugins:

- AdBlock
- HTTPS Everywhere
- Windows Defender Browser Protection
- no script

THANK YOU !

Abdullah Al Zmaili

Email: a.zmaili@zmaili.me

Mobile: 0785698163