# Cyber Awareness

Manish Lodha
Jt. Advisor,
Telecom Regulatory Authority of India (TRAI)

# Why is it easy to commit cyber crime?

Anonymity – Easy to remain anonymous

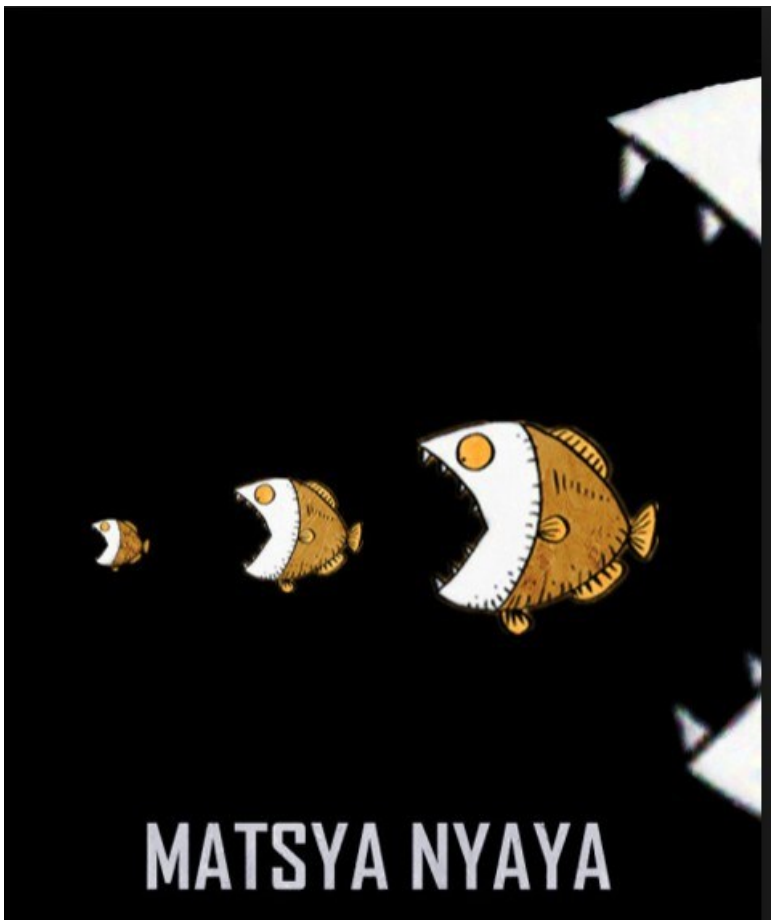
Inadequate legal jurisprudence - ability to commit crime from anywhere in the world

Easy availability of attack tools

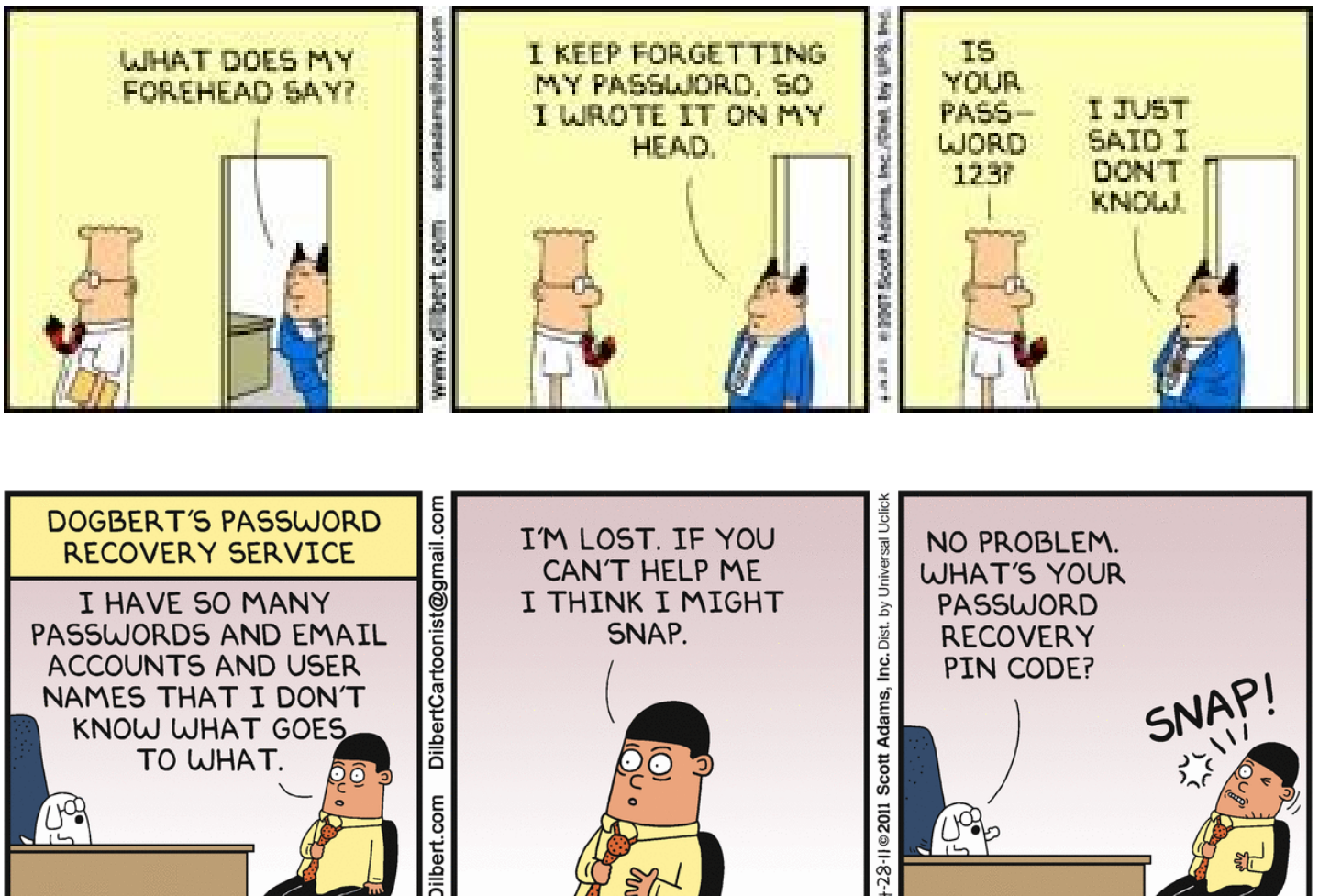
Virtual currency – easy to launder money

Rapid adoption of new technology

# Why is Cyber awareness important?



# Top 10 Tips

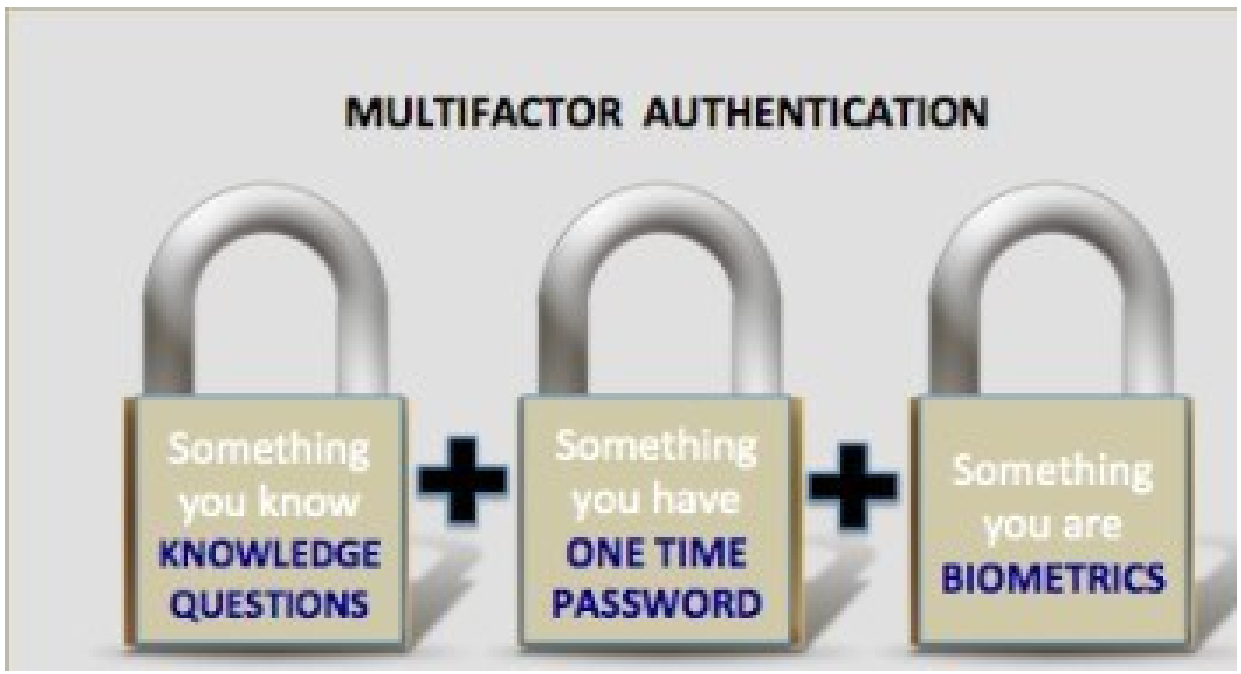

WHAT DOES MY FOREHEAD SAY?
I KEEP FORGETTING MY PASSWORD. SO I WROTE IT ON MY HEAD.
IS YOUR PASS-WORD 123?
I JUST SAID I DON'T KNOW.
DOGBERT'S PASSWORD RECOVERY SERVICE
I HAVE SO MANY PASSWORDS AND EMAIL ACCOUNTS AND USER NAMES THAT I DON'T KNOW WHAT GOES TO WHAT.
I'M LOST. IF YOU CAN'T HELP ME I THINK I MIGHT SNAP.
NO PROBLEM. WHAT'S YOUR PASSWORD RECOVERY PIN CODE?
SNAP!
www.dilbert.com scottadams@aol.com
Dilbert.com DilbertCartoonist@gmail.com
4-28-11 ©2011 Scott Adams, Inc. Dist. by Universal Uclick

# 1. Strong credentials

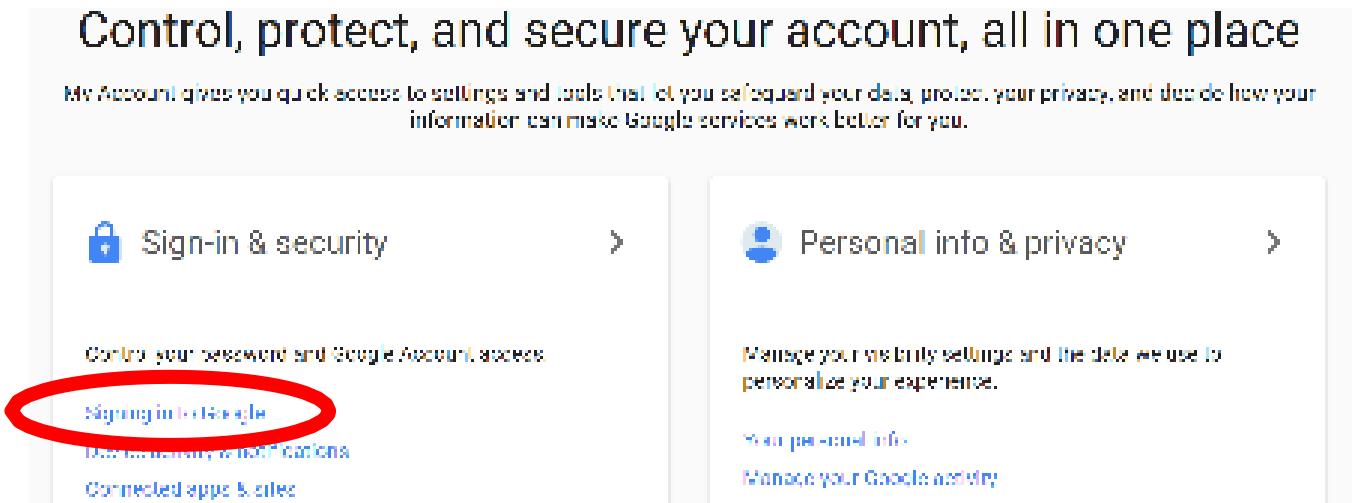
- Password hygiene
  - Have strong passwords
    - > 8 characters
    - combination of letters, numbers and special characters
  - Do not reuse passwords
  - Do not share passwords
  - Do not write passwords

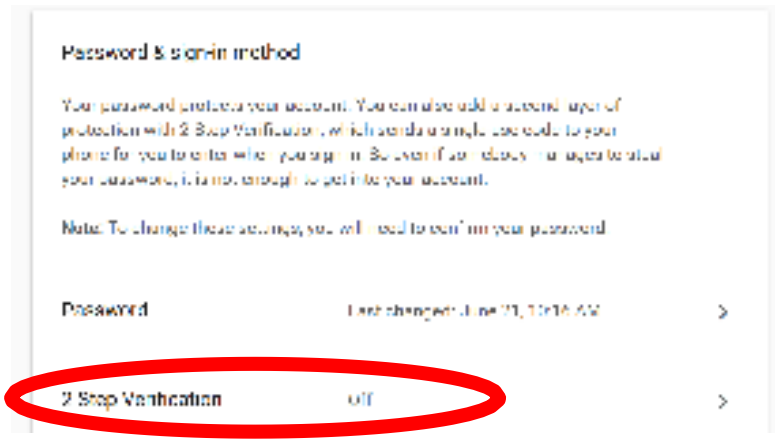
- Develop a method for password creation

# Multi-factor authentication

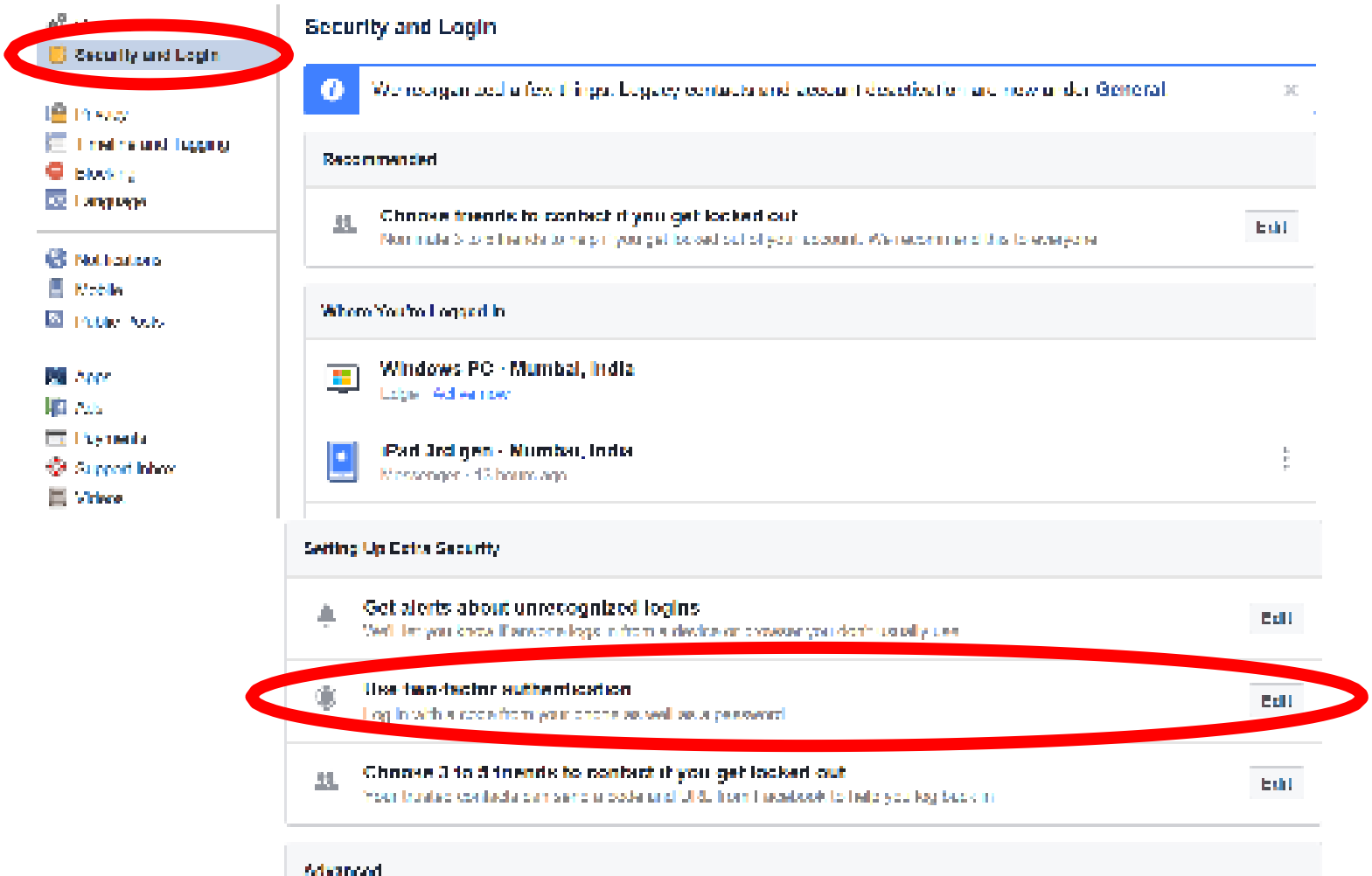


# How to enable multi-factor authentication



# How to enable multi-factor authentication



# 2. Backups

To obtain protection from…

Ransomware

Data corruption

Device damage / loss / theft

# 3. Updated and Active Anti-virus

- Verify it's running
- Verify it's updating virus definitions
- Verify it's scanning regularly

# 4. Keep all software up to date

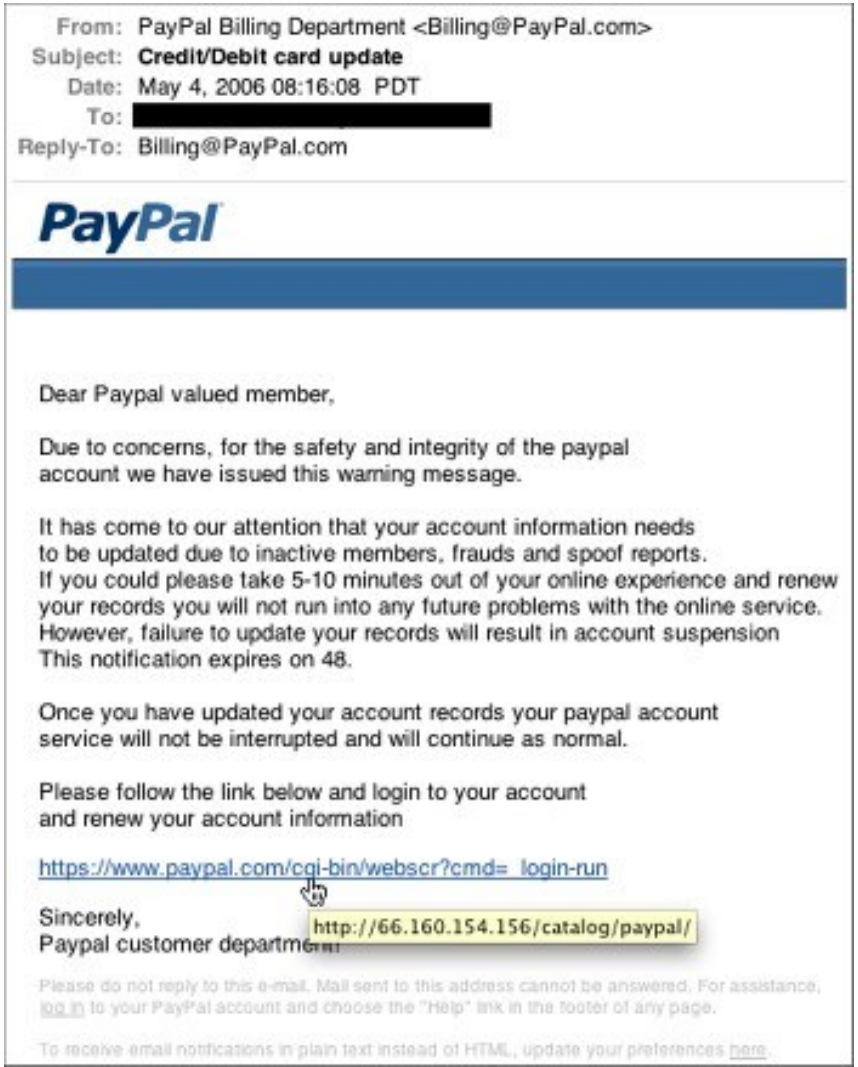
- OS
- Browsers
- Browser plugins
- Apps

# 5. Phishing

- Phishing
  - *Phishing* is the term for sending emails (considered the bait) with a link to a fake website. Once on the site, the user is tricked into giving sensitive information.

- Spear phishing
  - Phishing targeted at an individual, mostly someone senior in an organisation.

# Phishing examples



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Extra line breaks in this message were removed.

From: United Parcel Service of America [onlineservices@lufthansa.com] Sent: Mon 6/1/2009 5:00 AM
To:
Cc:
Subject: Postal Tracking #UY6LG72236FH1Y7

Message | UPSNR_976120012.zip (37 KB)

Hello!

We were not able to deliver postal package you sent on the 14th of March in time because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office.

Your United Parcel Service of America

# Phishing cheatsheet

1. Did you expect this?
2. Did it identify you? Or is it asking you to identify yourself?
3. Are there spelling / grammatical mistakes
4. Observe the email id – both displayed as well as actual email id
5. Do not trust URL text; see the URL carefully by hovering over
6. Do not click on the URL; login to the legitimate site directly
7. Do not go by look and feel
8. Check full URL of shortened URLs
9. Be wary of unsolicited attachments
10. Is it trying to bait you with urgency?

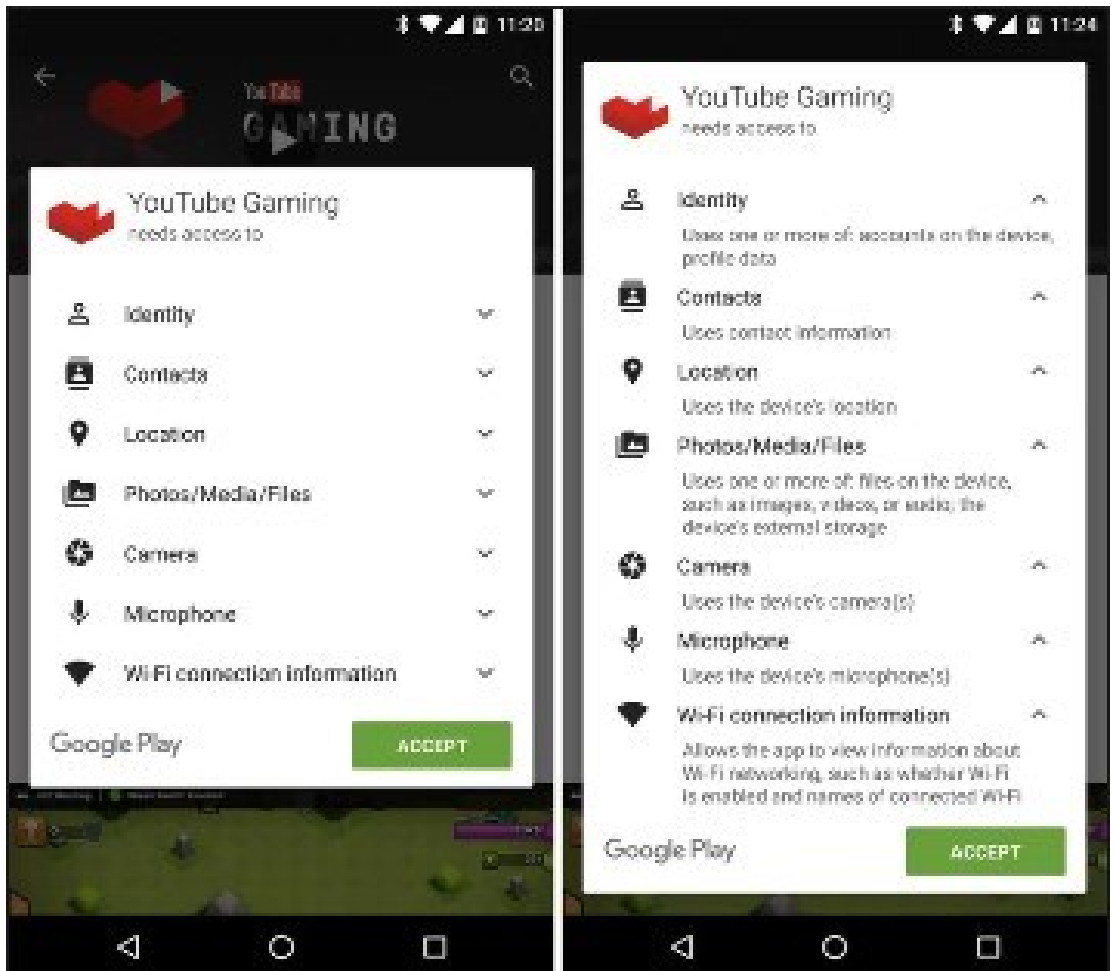
# 6. Careful what apps you install…

- Install from trusted app store
- Install from the original organisation

# …and what apps are already installed!

- What data is it collecting?
- Where is the data transferred?
- What is the data used for?
- How long is the data stored?

# 7. Review data access of apps



# 8. Share minimum data on social media

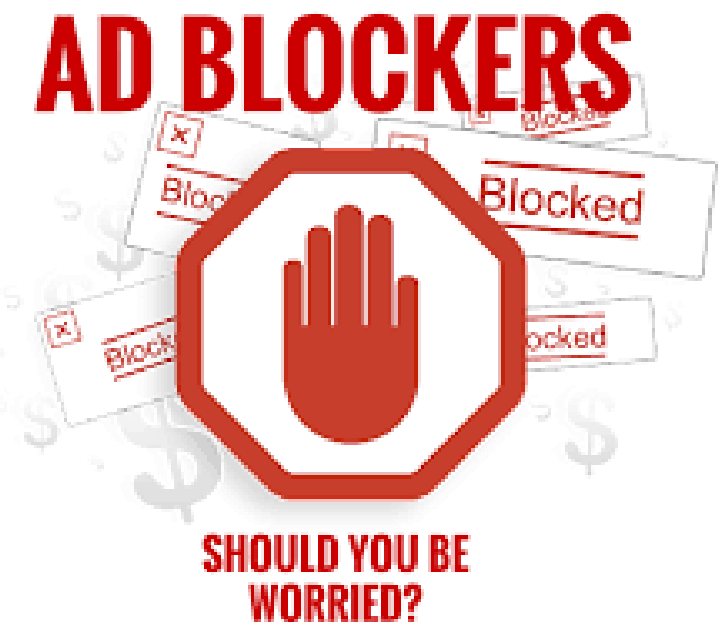
Careful with PII and social data

- Date of birth
- Living address
- Names of family members
- Phone number
- Email address
- School
- Vacation plans

# 9. Avoid using public hotspots

- Especially if you are browsing http sites

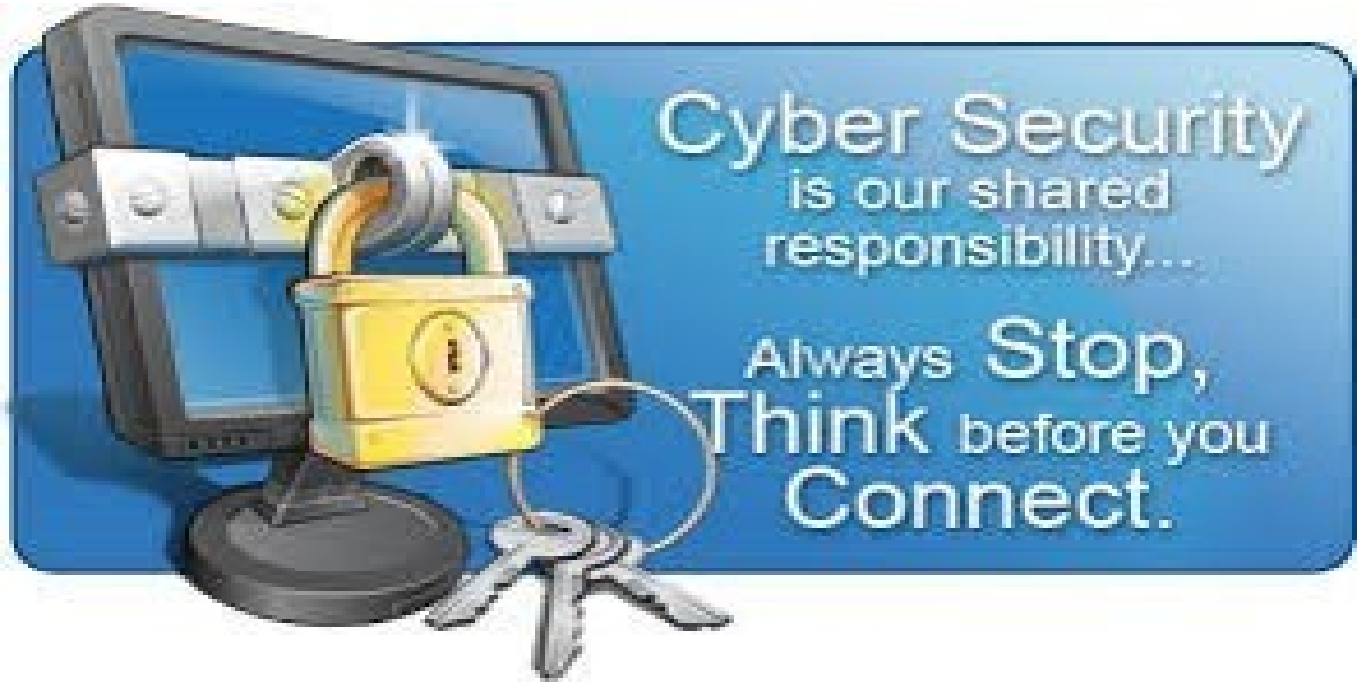
# 10. Use ad blocker




- Malwares are injected through malicious ads
- Ad servers track your browsing

# Cyber awareness - Top 10 Tips

| S.No. | Tip |
|---|---|
| T#1 | Strong credentials |
| T#2 | Backup data |
| T#3 | Keep anti-virus up to date |
| T#4 | Keep all software up to date |
| T#5 | Beware of phishing |
| T#6 | Fake mobile apps…and factory built apps |
| T#7 | Review data access of apps |
| T#8 | Share minimum data on social media |
| T#9 | Avoid using public hotspots |
| T#10 | Use ad blocker |


Cyber Security
is our shared
responsibility...
Always Stop,
Think before you
Connect.

Thank you