

# 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

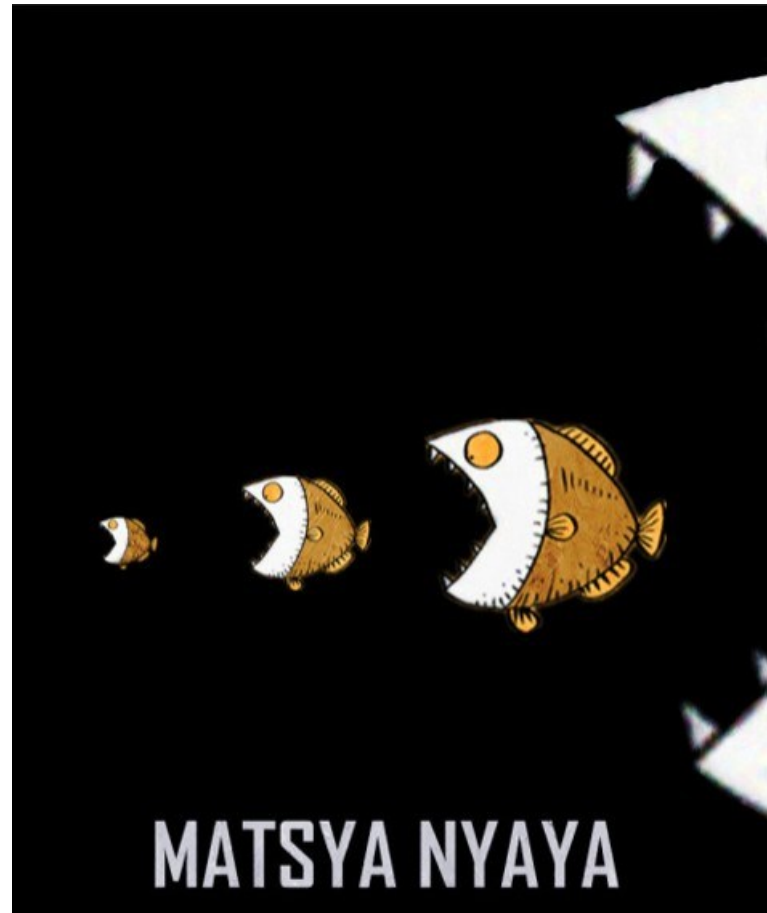


Virtual currency – easy to launder money

Rapid adoption of new technology



# Why is Cyber awareness important?

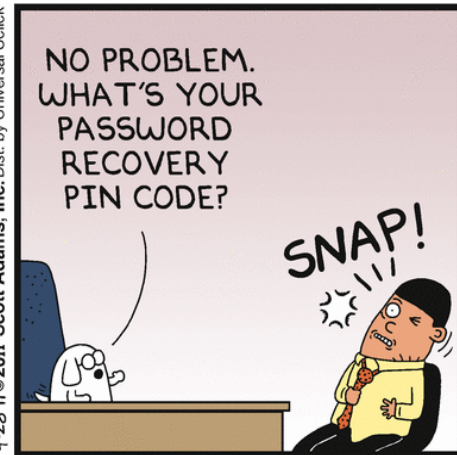


# Top 10 Tips



www.dilbert.com

© 2007 Scott Adams, Inc./Dist. by UFS, Inc.



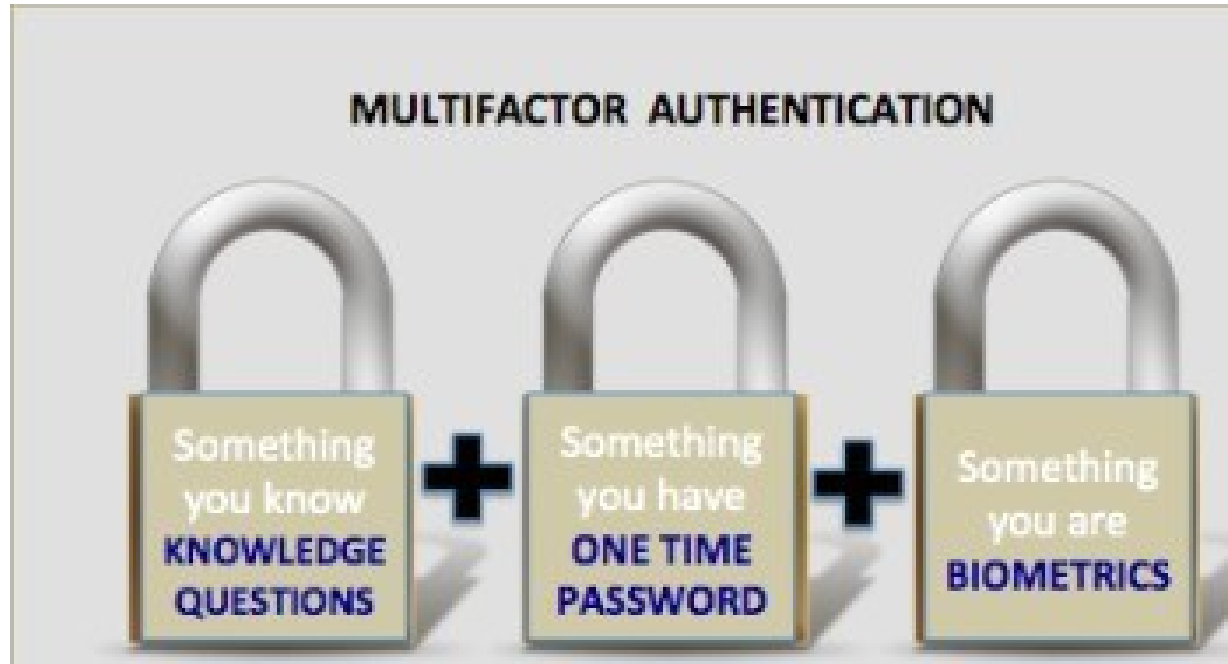
Dilbert.com DilbertCartoonist@gmail.com

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

Google



[Click here to enable desktop notifications for Gmail.](#) [Learn more](#) [Hide](#)

Gmail ▾

Settings

COMPOSE

General Labels Inbox Accounts and Import Filters and Blocked Addresses

Offline Themes

Setup progress:

10%



My Account



Search



Maps

## Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.



Sign-in & security >

Control your password and Google Account access.

[Signing into Google](#)

[Device activity & notifications](#)

[Connected apps & sites](#)



Personal info & privacy >

Manage your visibility settings and the data we use to personalize your experience.

[View personal info](#)

[Manage your Google activity](#)

### Password & sign-in method

Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if someone has figured out your password, it is not enough to get into your account.

Note: To change these settings, you will need to confirm your password.

Password

Last changed: June 11, 10:16 AM



2-Step Verification

off





# How to enable multi-factor authentication

The image shows the Windows Settings application, specifically the 'Security and Login' section. The left-hand navigation pane has 'Security and Login' highlighted with a red circle. The main content area is titled 'Security and Login' and contains several sections. A red circle highlights the 'Use two-factor authentication' option under the 'Setting Up Extra Security' section. The text for this option reads: 'Log in with a code from your phone as well as a password'. Other options include 'Get alerts about unrecognized logins' and 'Choose 3 to 5 friends to contact if you get locked out'.

**Security and Login**

We reorganized a few things. Legacy contacts and account identification are now under General.

**Recommended**

Choose friends to contact if you get locked out  
Name: Mike & Lisa | Email: mike@xyz.com | You get locked out of your account. We recommend this to everyone. [Edit](#)

**Where You've Logged In**

Windows PC - Mumbai, India  
[Log out](#) [Add a new](#)

iPad 3rd gen - Mumbai, India  
Microsoft Edge - 15 hours ago

**Setting Up Extra Security**

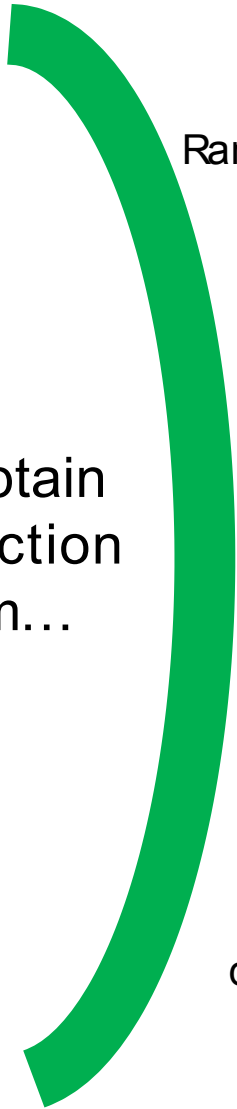
Get alerts about unrecognized logins  
Get notified when you know if someone logs in from a device or browser you don't usually use. [Edit](#)

**Use two-factor authentication**  
Log in with a code from your phone as well as a password. [Edit](#)

Choose 3 to 5 friends to contact if you get locked out  
Your trusted contacts can send a code to you from Facebook to help you log back in. [Edit](#)

**Microsoft**

# 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



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

Sincerely,  
Paypal customer department


<http://66.160.154.156/catalog/paypal/>

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

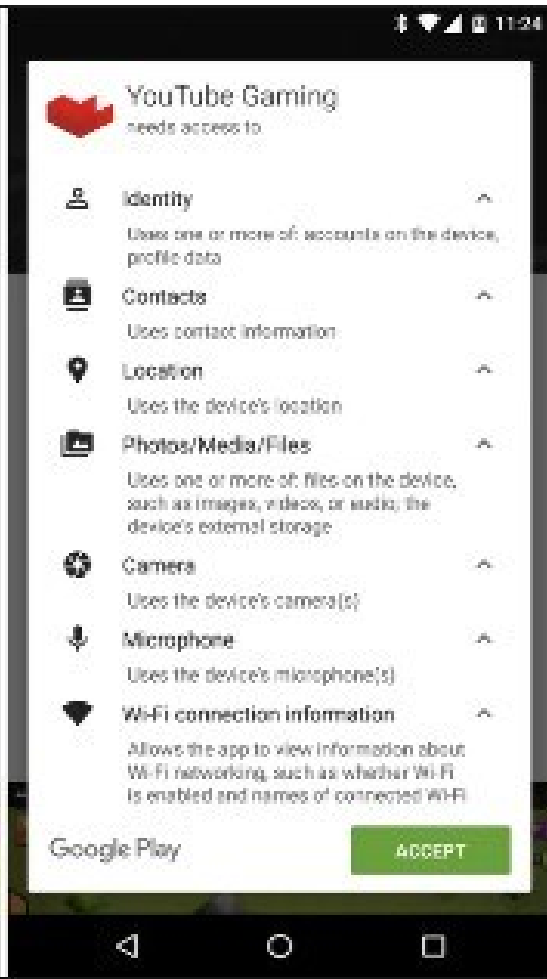
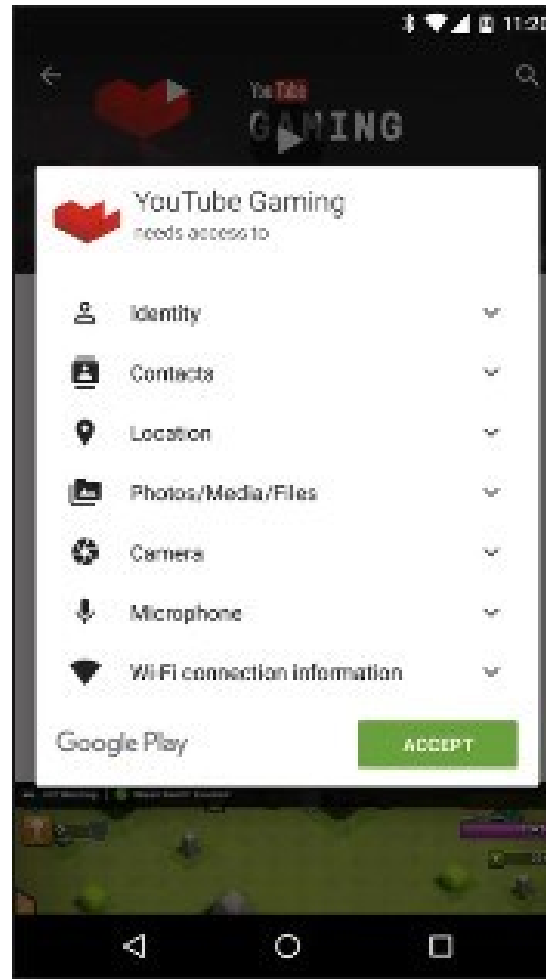


# ...and what apps are already installed!

- 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

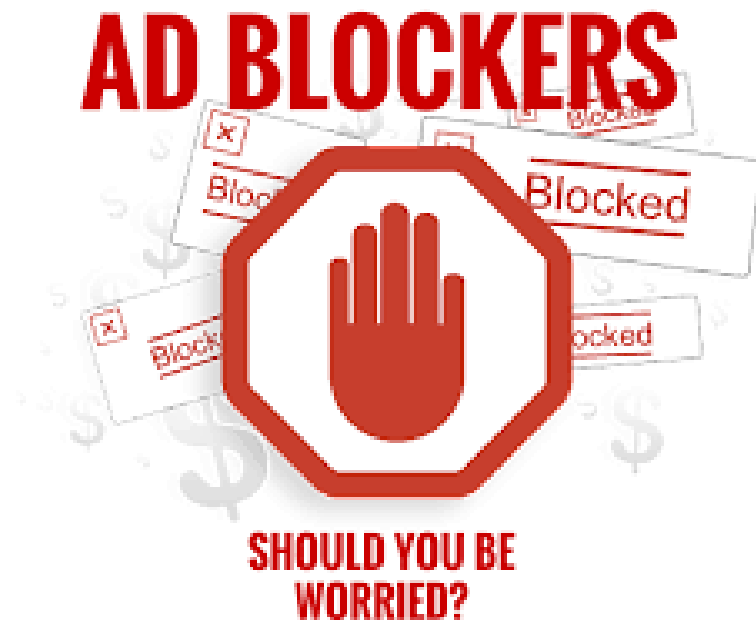
- Date of birth
- Living address
- Names of family members
- Phone number
- Email address
- School
- Vacation plans

## 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



Thank you