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

Virtual currency – easy to launder money

Easy availability of attack tools

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 PASSWORD 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!!
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

1. Open Facebook and go to the "Security and Login" section.
3. Follow the instructions to set up two-factor authentication using a code from your phone as well as a password.
2. Backups

To obtain protection from...

- Ransomware
- Data corruption
- Device damage / loss / theft

BACKUP YOUR STUFF
Before It’s Too Late!
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]

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

Sincerely,
Paypal customer department

http://66.160.154.156/catalog/paypal/

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

---

From: United Parcel Service of America [onlineservices@upshansa.com]
Sent: Mon 6/1/2009 5:00 AM
To: [REDACTED]

Subject: Postal Tracking #UV6G72236FHV17

Extra line breaks in this message were removed.

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