Cyber Safety Handout

Be cyber safe!

Building a better working world

Contents

Acronyms

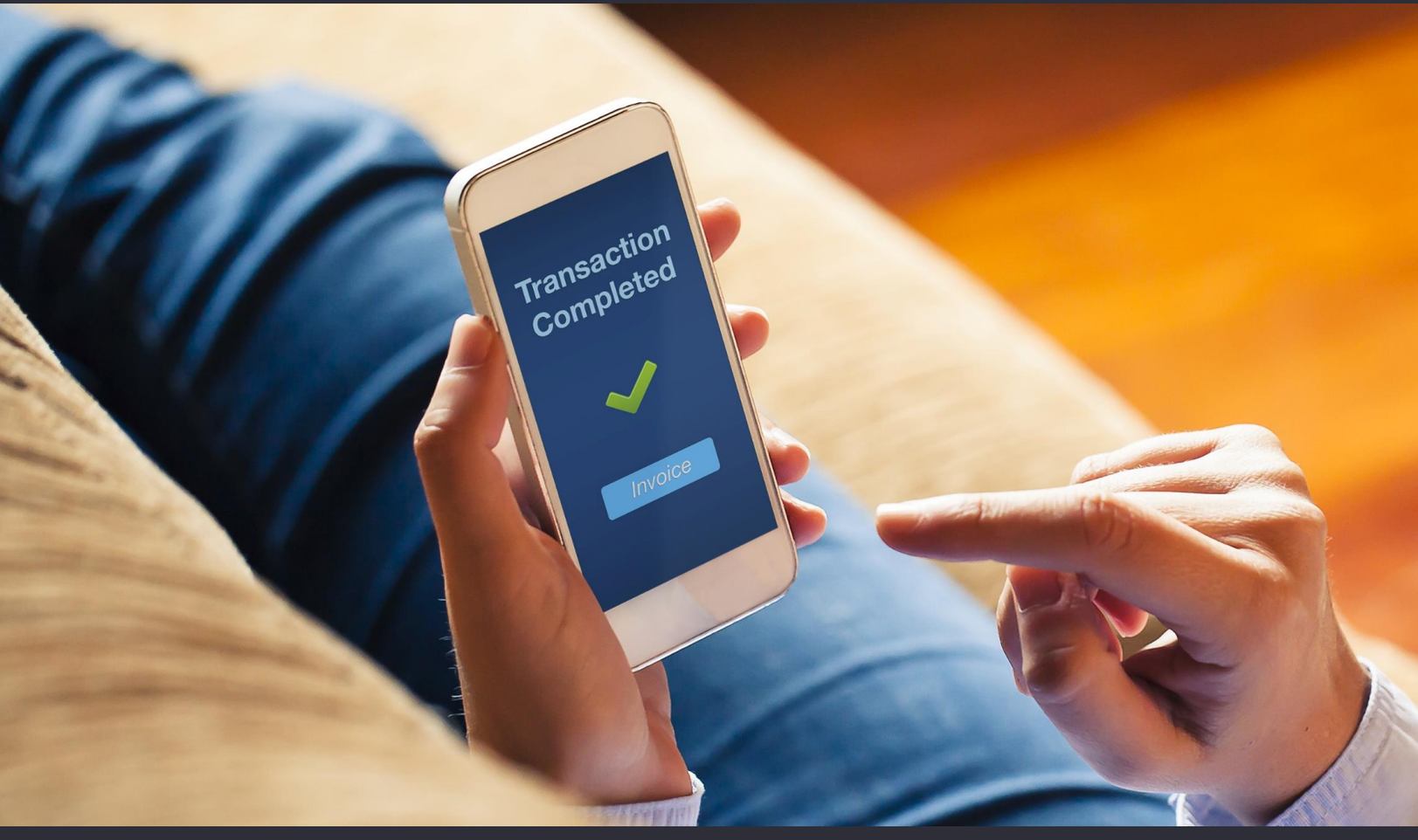
2FA	Two-factor authentication
CVV	Card Verification Value
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity document
IT	Information Technology
NCRB	National Crime Records Bureau
OS	Operating System
OTP	One-time password
PIN	Personal Identification Number
URL	Uniform Resource Locators

About cyber safety handout

We are living in the digital age of emerging technology which has changed the modern way of life. Today, internet has eased the use of communicating with friends, searching and sharing information, performing financial transactions, and even running entire businesses online. The internet has offered a lot and made our lives simpler. However, its open and unregulated nature makes us vulnerable to a wide range of threats.

In recent times, there has been an upsurge in crimes in the cyber world. Cyber crime has become a menacing reality in India, majorly affecting women and children. Cyber crime now is not just limited to hacking but it also includes stalking, defamation, bullying, extortion, harassment, trolling, frauds, terrorism and phishing attacks. Most of these crimes are difficult to detect and rarely reported. There is still lack of awareness among people which keeps these cyber criminals at an advantageous position.

This handout helps citizens, especially women and children, in understanding the realities of the cyberworld and preparing themselves in becoming informed users of the internet.



Cyber story

Credit/debit card fraud

Riya receives a call from an unknown phone number.

Caller: Ma'am I am Mukesh from your bank, we have seen some unusual activity on your credit card. I will ask some card–related questions to ensure that it is safe to use.

Riya: Ok sure, I hope there is nothing serious.

Caller: Ma'am don't worry we will sort this out. Now, can I know your full name?

Riya: Yes, its Riya Jain.

Caller: Can I know your card number and CVV number, for validation?

Riya: Ok, card no. is 4321 XXXX XXXX XX11 and CVV is 7XX

Caller: Thank you, Ma'am. Now you must have received an OTP on your registered number. Can you please share that?

Riya: Yes, its 121 323.

Caller: Thank you, Ma'am. Your verification has been successful. Thank you for your time.

Riya: Thank you so much.

Within the next 2 minutes, a transaction of INR 1 lakh was made from her credit card. Riya became a victim of credit card fraud.

Cyber story learnings

Credit/debit card fraud

A lot of people are becoming victims to credit card frauds where they fall prey to the psychological traps of the attackers. The attackers either lure the victims by providing them with lucrative offers or scare them by providing false information regarding their credit/debit cards. The attacker takes the advantage of the victim's vulnerable position and extracts sensitive information (such as name, bank account details, Aadhaar details, etc.) from them.

Credit/Debit card frauds majorly take place over phone calls, emails, and SMSs, therefore it is important that we become more vigilant and aware while sharing any kind of information.

Quick Learnings

- Do not get scared if you receive a call stating that your card is blocked. Bank will never convey such information on the call.
- Do not share your PIN, password, card number, CVV number, OTP etc. with any stranger, even if he/she claims to be a bank employee. The bank is never going to ask for any vital information.
- Always have your bank's customer service number on hand so you can report any suspicious or unauthorized activity on your account right away.
- Never share your bank related/ financial information over phone with unidentified callers.

1 Importance of cyber security awareness

Nowadays, technologies like the internet, computers and phones have, etc. has taken on a vital role in our lives. A day without using any of these digital devices is unthinkable. Even after spending so much time surfing the internet, we are still unaware of the importance of cybersecurity. With new and powerful cyber–attacks striking the internet regularly, we must be vigilant while making use of technology to reduce the risk of cyber threats.

60.8%

of cybercrimes cases registered with NCRB in 2021 were for the motive of fraud

NCRB registered

52,974

Cases under cybercrime in 2021

NCRB registered

4,555

cyber cases across states with sexual exploitation motivation 2021

NCRB registered

8,513

Computer Related Offences in 2021 across 19 metropolitan cities

10,730

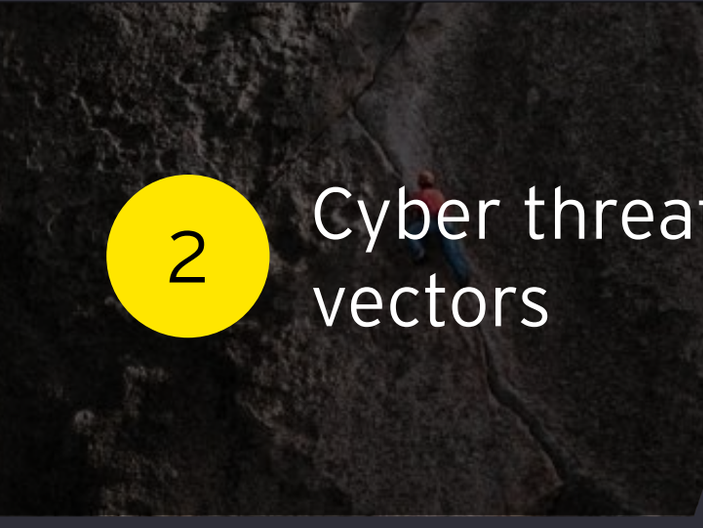
cybercrimes registered against women in 2021 which includes cyber blackmailing, defamation, cyber pornography, fake profile, etc.

1,376

cybercrimes registered against children in 2021 which includes child pornography, threatening, bullying, internet crimes through online games, etc.

The most common target for cyberbullies are children, young adults (especially girls) and students. Juice jacking, loan app scams are emerging and prevalent cybersecurity threats.

Reference: https://ncrb.gov.in/en/node/3721



2 Cyber threat vectors

Reference: https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf

Email spoofing

Email spoofing is a fraudulent email activity of forging an email address to make it look like it has been sent from a genuine source.

Social engineering

Social engineering is a technique used by cybercriminals to deceive and manipulate individuals into sharing personal or confidential information.

Cyberbullying and harassment

Cyberbullying is the practice of bullying individuals online. It is a form of harassment, intimidation or threat inflicted online through platforms such as social media, gaming and messaging.

Identity theft

Identity theft is the act of wrongfully obtaining and using someone else's identity (personal or financial information) to gain benefits in other person's name.

Malicious files applications

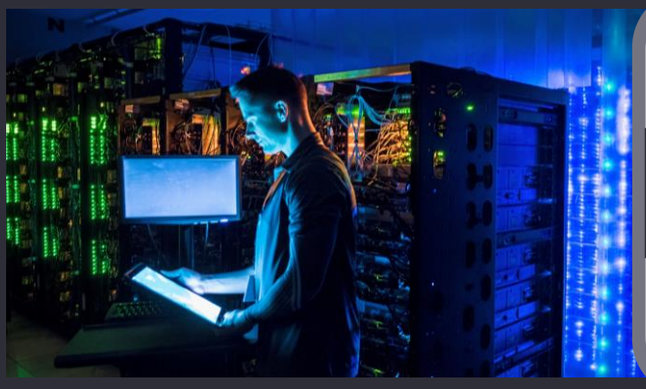
Malware or malicious software, is a program or file that comes from emails, messages, gaming, website, etc. It compromises user security, steals, encrypts or deletes sensitive data on your computer or other devices.

Online frauds

Online fraud can be in many forms like financial or banking fraud, social media fraud, job fraud, lottery scams, phishing email scams, fake antivirus software, profile hijacking, auction fraud, etc.

Cyber threat vectors

Minimizing risk exposure



Malware

Malware or malicious software, is a program or file that that damages or performs unwanted actions on a computer system and compromises user security. It could steal, encrypt or delete sensitive data on your computer or other devices.

Quick tips

- **Keep software up to date.** Attackers know about weaknesses in the software on your device before you do.
- **Back up data** as no one ever thinks they will be hacked until they do.
- **Do not pay the ransom.** You might get asked to pay repeatedly without any resolution to your issue.
- **Contact IT support** if you have clicked or downloaded something suspicious.

Internet Browsing

54% of Phishing sites use HTTPS to trick users

HTTP website are ***safe to view only***. Since, your connection is not secure the information you send or receive to the website can be intercepted.

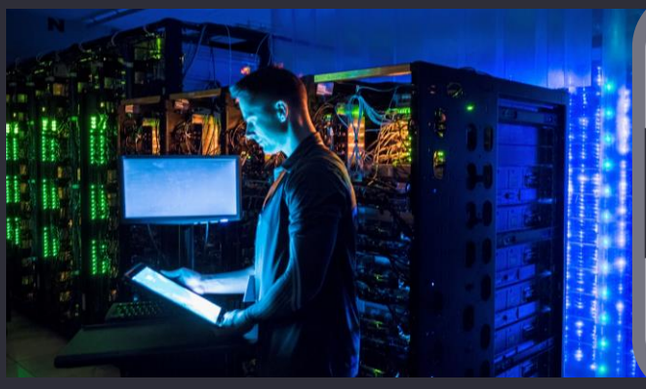
The S stands for secure. Therefore, if you need to enter sensitive information such as passwords, credit card or any other personal details, you need to ensure the ***site is secure with HTTPS***

In the absence of HTTP or HTTPS the website is considered to be ***unsafe to view or transmit information*** and is best to avoid such websites.

Reference: https://community.webroot.com/news-announcements-3/the-2021-webroot-brightcloud-threat-report-54-of-phishing-sites-use-https-to-trick-users-347178

Cyber threat vectors

Social engineering

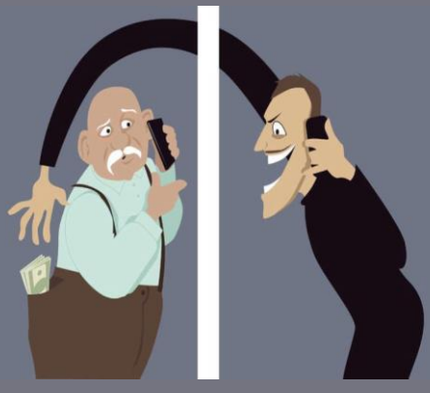


Social engineering

People are the weakest link in security, it's easier to exploit someone's trust than it is to hack a computer. Hackers use social engineering techniques to gain your confidence to get sensitive information from you. This can be done over calls, emails, messages, etc.

Quick tips

- **Be suspicious of unknown callers.** Avoid answering calls from numbers not stored on your contact list
- **Do not trust Caller ID.** Just because the screen displays a legitimate name does not mean the caller is legitimate.
- **Call back.** In case you already had a conversation and doubt about it, call them back on the same number and check.



- **Ask questions, probe.** No one known to you will ever ask for your personal or financial information.
- **Do not call a number sent in a voicemail,** text or email unless you are sure of the sender.
- **Do not share information,** over calls or messages if you are not sure about the legitimacy of the caller.

Reference: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Cyber threat vectors

Phishing emails

Phishing is a cybercrime carried out mostly through emails, phones or text messages, where the attacker poses as a trusted person to target potential victims into providing sensitive data such as personal information, financial information, passwords, etc. which can thus be used to access or hack into important accounts and can result in identity theft and financial loss.

1. Dating back to the 1990s, phishing is one of the oldest
2. Increase in the COVID-19 related phishing and ransomware attacks
3. Increased security risk from remote working/learning
4. Over 3 billion emails a day phishing scams emailed each day

Spotting a phishing email

- **Suspicious attachment** request to open attachments to check and verify data.
- **Sense of urgency**. Phishing emails will usually use a language that demands for immediate actions.
- **Hyperlinked URL** differs from the title name displayed and the link is shortened.
- **Personally identifiable information.** Requests for personal information like username, financial transactions.
- **Spelling errors** (e.g., "pessward"), lack of punctuation marks or poor use of grammar.

Reference:
https://www.phishing.org/history-of-phishing
https://cmte.ieee.org/futuredirections/2022/02/06/3-billion-phishing-email-every-day/#:~:text=It%20turns%20out%20that's%20not,every%20single%20day%3A%203%20billion!

Cyber story learnings

Password security

The advancements in technology has led to the increasing use of computing devices such as mobiles, laptops, computers, etc . All these machines are susceptible to misuse by unauthorized users, who can gain access into your systems.

Therefore, users should always protect their systems with strong passwords to ensure the safety and security of sensitive data.

Quick Learnings

- **Complex.** Use difficult passwords which are at least 8 characters long with a combination of numbers and symbols
- **Default.** Change the initial/default password immediately after the first log on
- **Don't.** Do not store passwords in digital or physical form and do not share it with anyone
- **2FA.** Enable 2 Factor Authorization for all your accounts—along with passwords, also generate a Mobile PIN
- **Change.** Change passwords at regular intervals and avoid using same passwords in periodically and for multiple platforms

Reference: https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf

3 Securing yourself

Summary of tips

Malware prevention

1

Be careful while you click on links. Have a good backup of your data. Never plug unknown USBs into your system. Do not use pirated software.

Never do banking transactions on public Wi-Fi. Also, do not log-in to your email accounts from public computers.

2

Stay secure

Phishing-that's how hackers break in!

3

Be careful with email attachments and links. Do not share sensitive information over emails. Scammers exploit your trust, be watchful.

It takes only 1 click on the wrong link to open the wrong file and hackers can gain complete control of your computer. Avoid clicking on links sent by strangers/unknown mail IDs.

4

One click, hackers in!

Mobile menace

5

Only install applications from the trusted app store, keep your phone updated with the latest software upgrades and turn-off Bluetooth, AirDrop and Wi-Fi when not in use.

Use strong and long passwords, short complex passwords are of little use. Don't use the same passwords for different accounts and applications. Change them regularly.

6

Passwords-good practices

Email security

7

Two-factor authentication is an increasingly popular and effective way to protect the security of your accounts-so start using it for both official and personal accounts.

3 Securing yourself

Summary of tips

Beware of fakes 8 Only buy on sites, online store pages, and applications you know. For online websites, it should have HTTPS. The "s" means that it is secure.

Regularly log out of applications and devices, especially for sites that hold your personal and/or financial information. 9 **Log in–log out**

Keep privacy settings high 10 Keep privacy settings high on social networks to prevent sensitive information from being shared with the public.

Format/destroy/shred important documents, CDs, and hard disk before disposing them. 11 **Format/destroy before disposing**

Secure downloads 12 Download the app only from the official app store. Check app reviews and ratings to verify the authenticity before downloading.

Regularly update Operating Software (OS) and all other applications on all devices. Delete all unused applications. 13 **Regular updates**

Got hacked–now what? 14 Immediately inform your IT Team and follow their guidelines. Avoid any interaction with the affected computer–disconnect completely.

Be cyber safe

Find out more...

Key Contacts

Murali Rao

Cybersecurity Consulting Leader, EY India
+91 9945178672
murali.rao@in.ey.com

Rahul Rishi

Gov and Public Sector–Africa India Middle East–Consulting Leader
+91 9811999050
rahul.rishi@in.ey.com

Honnur Muralidhara

Partner, Technology Consulting, EY India
+91 9845596748
muralidhara.hc@in. ey.com

Krishna P

Sastry Partner, Cybersecurity, EY India
+91 9490433296
Sastry.Pendyala@in .ey.com

Navin Kaul

Partner, Cybersecurity, EY India
+91 9971496366
navin.kaul@in.ey.com

Murari Sharma

Manager, Cybersecurity, EY India
+91 9816411017
murari.sharma@in.ey.com

Jyoti Thakur

Senior Consultant, Cybersecurity, EY India
+91 9857637000
jyoti2.thakur@in.ey.com

Yamini Sharma

Consultant, Cybersecurity, EY India
+91 8219084883
yamini.sharma@in.ey.com

Our offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
11, Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurugram - 122 002
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur – 831 001
Tel: + 91 657 663 1000

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune
C-401, 4th floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

AK1

ey.com/en_in

@EY_India EY EY India EY Careers India @ey_indiacareers