राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान, रोपड़

National Institute of Electronics and Information Technology (NIELIT), Ropar

SOCIAL NETWORK SECURITY

RAMINDER SINGH

SCIENTIST ‘E’, NIELIT

Roadmap of the Presentation

- Social Network Security
- Password Attacks
  - Password Attack Mitigation
- Phishing
  - Phishing detection & Avoidance
- Malware Propagation
- Understanding Browser Security
- Protecting yourself when using social media
- Remote Access Scam/Tech Support Scam
- Cyber Law
  - Indian IT Act 2000
  - Some Important sections in IT Act
  - The IT Amendment Act 2008 and its details

Social Network Security

- collection of guidelines and practices known as "social media security" guards user data, accounts, and privacy on social networking sites.
- offers protection from identity theft, malware, phishing attacks, unauthorized access, online harassment, and data breaches.
- Security on social media is crucial for both individuals and corporations. It can support safeguarding executives' social media presence and a brand's credibility.

Password Attacks

An attempt to obtain or decrypt a user's password for illegal use. Hackers can use cracking programs, dictionary attacks, and password sniffers in password attacks. Defence against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes.

Mitigating Password Attacks

Update Password

- It’s always a great idea to keep changing essential passwords in regular intervals
- Passwords shouldn’t be the same for everything

Use Alpha-Numeric

- When setting a password general best practices should be followed
- A password should contain a multitude of characters with a generous use of alpha numeric

NO Dictionary

- It’s always a great idea to use a password that only makes sense to you
- Passwords which use actual words that make sense are much more susceptible to dictionary attacks

Phishing Mitigation Cheat Sheet

- Did you expect this?
- Do you know the email id
- Confirm over phone

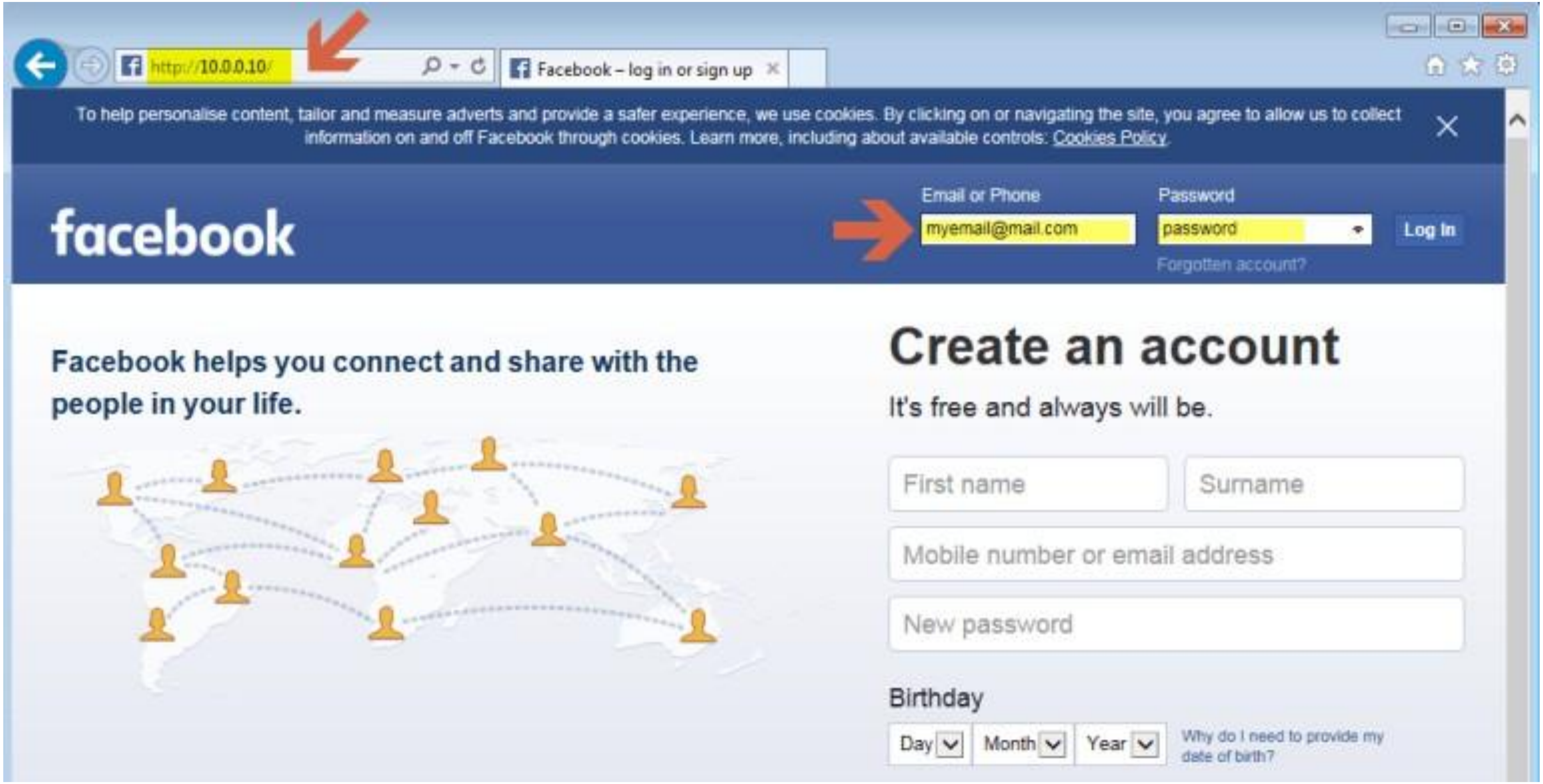
- Does it have any attachments
- Does it have any external links
- Hover over the link

Look for

- Urgency
- Personal Information
- Penalty

- Phone Number
- Too much Personal Information
- Spelling mistakes

Avoid Phishing Websites



http://10.0.0.10/

Facebook – log in or sign up

To help personalise content, tailor and measure adverts and provide a safer experience, we use cookies. By clicking on or navigating the site, you agree to allow us to collect information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.

facebook

Email or Phone: myemail@mail.com

Password: password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

New password

Birthday

Day | Month | Year

Why do I need to provide my date of birth?

DOs to mitigate Phishing Attacks

- Do not open other Internet browser sessions and access other websites while you are performing online financial transactions/enquiry through the Internet. Remember to print or keep the copy of transaction record or confirmation notice for checking.
- Always be wary when giving off sensitive personal or account information. Banks and financial institutions seldom ask for your personal or account information through email. Consult the relevant organisation if in doubt.
- Always ensure that your computer is applied with the latest security patches and anti- malware software with updated definition file to reduce the chance of being affected by fraudulent emails or websites riding on software vulnerabilities. This also helps to protect your computer from other security or malware attacks.
- Consider using desktop spam-filtering products to help detecting and blocking scam emails but beware of false alarms. Learn the technical abilities that are essential for deploying these products in an effective manner.

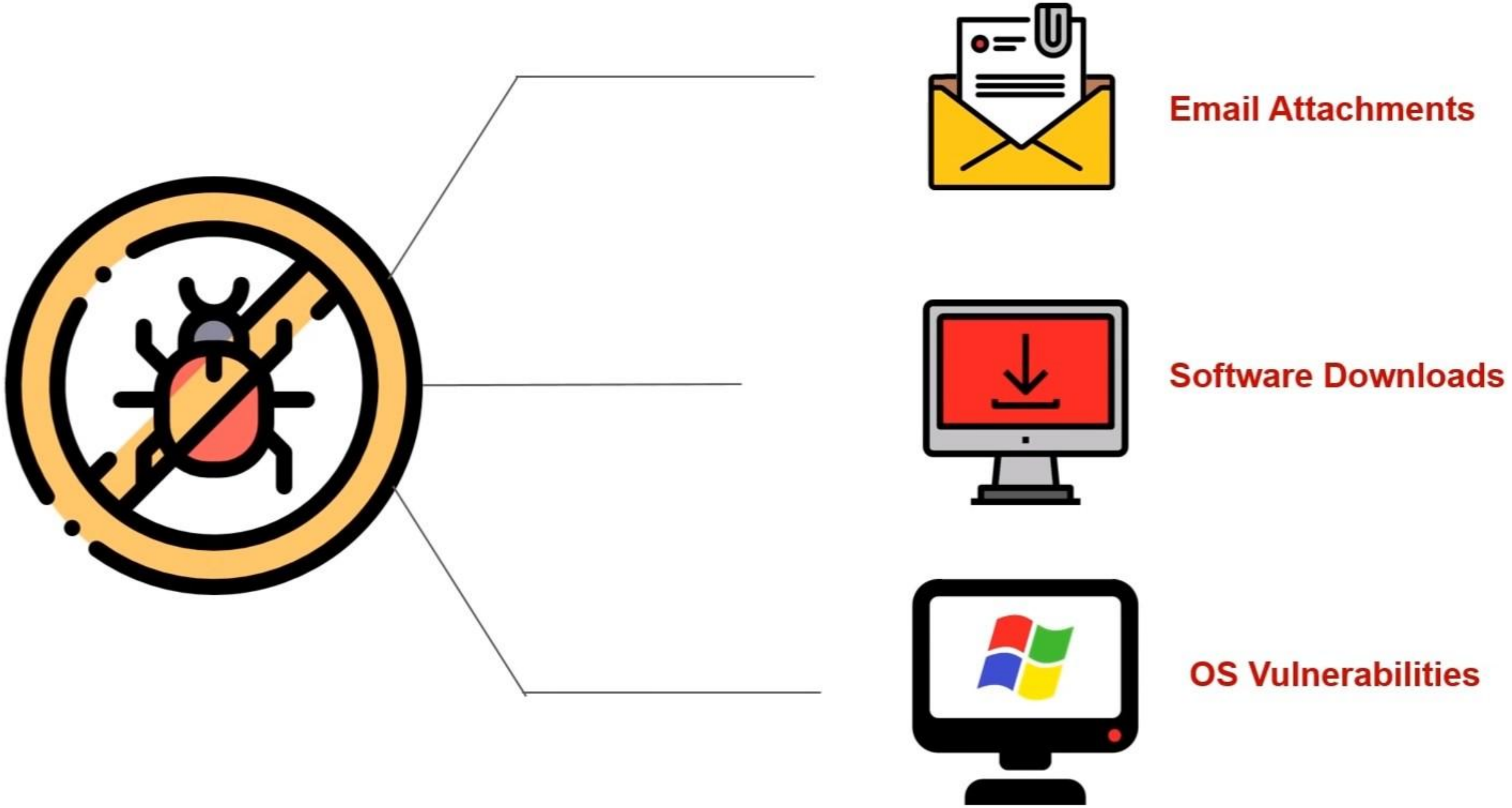
Phising - Detection

- Review your credit card or bank account statements as soon as you receive them to check for any unauthorised transactions or payments.
- Log into your accounts regularly to check for the account status and last login time to determine whether there is any suspicious activity.
- Verify the legitimacy of the website of an organisation such as banks by contacting the organisation through its address or telephone number.

Phishing Response

- Change the password immediately if you suspect that you have already been defrauded (e.g. responded to phishing emails or supplied your personal/financial information to the fraudulent websites).
- Check your account status and contact the relevant organisation / response team immediately.
- Send the phishing emails to your IT security team and/or the police for their investigation.

Malware propagation



Email Attachments

Software Downloads

OS Vulnerabilities

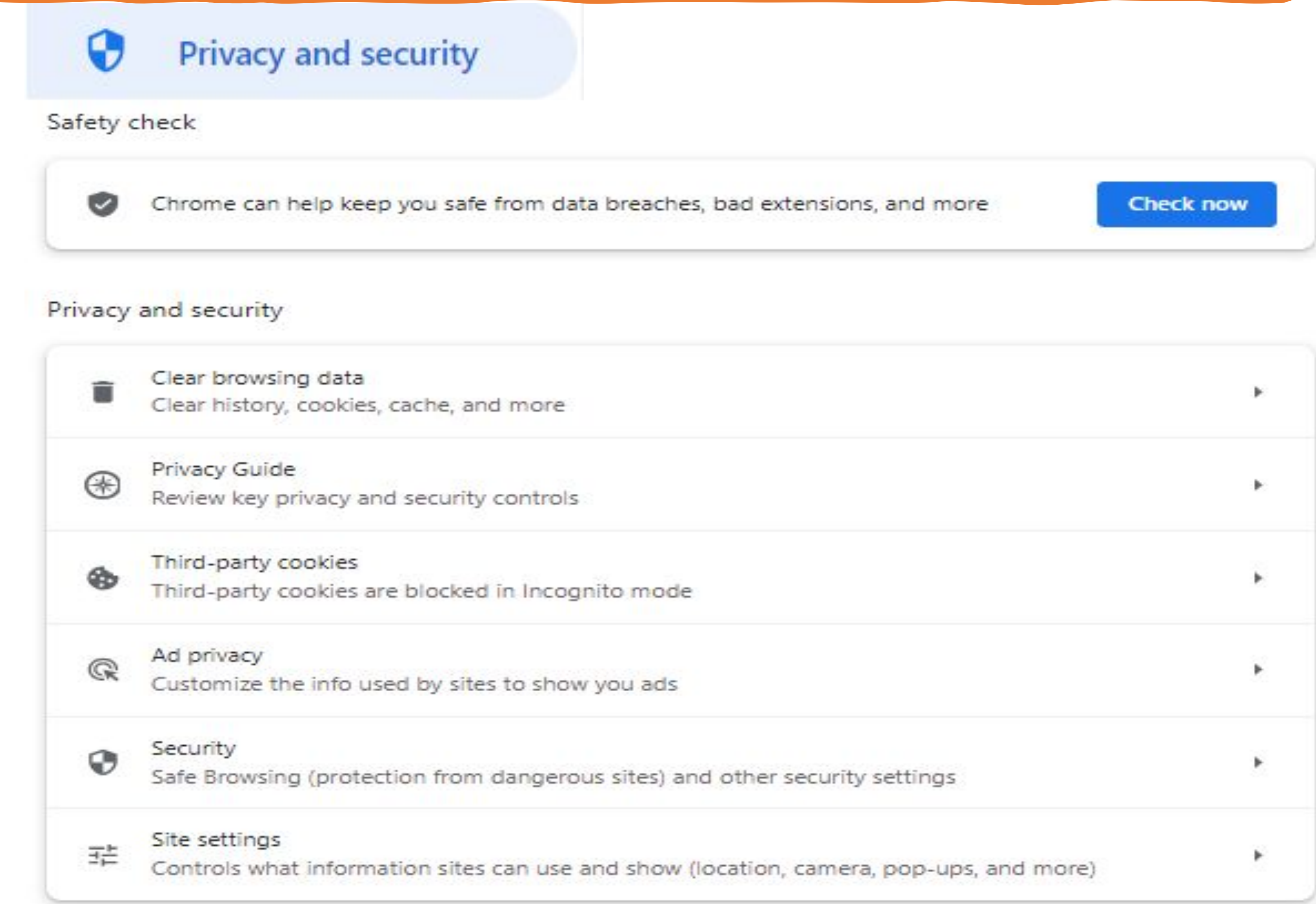
The NEVER EVER option to be exercised

Ascertain genuineness of software as well as genuineness of sites offering software prior to downloading it.

Please Remember

“NOTHING is FREE ON TH INTERNET”

Understanding Browser Security



Privacy and security

Safety check

Chrome can help keep you safe from data breaches, bad extensions, and more

Privacy and security

Clear browsing data
Clear history, cookies, cache, and more

Privacy Guide
Review key privacy and security controls

Third-party cookies
Third-party cookies are blocked in Incognito mode

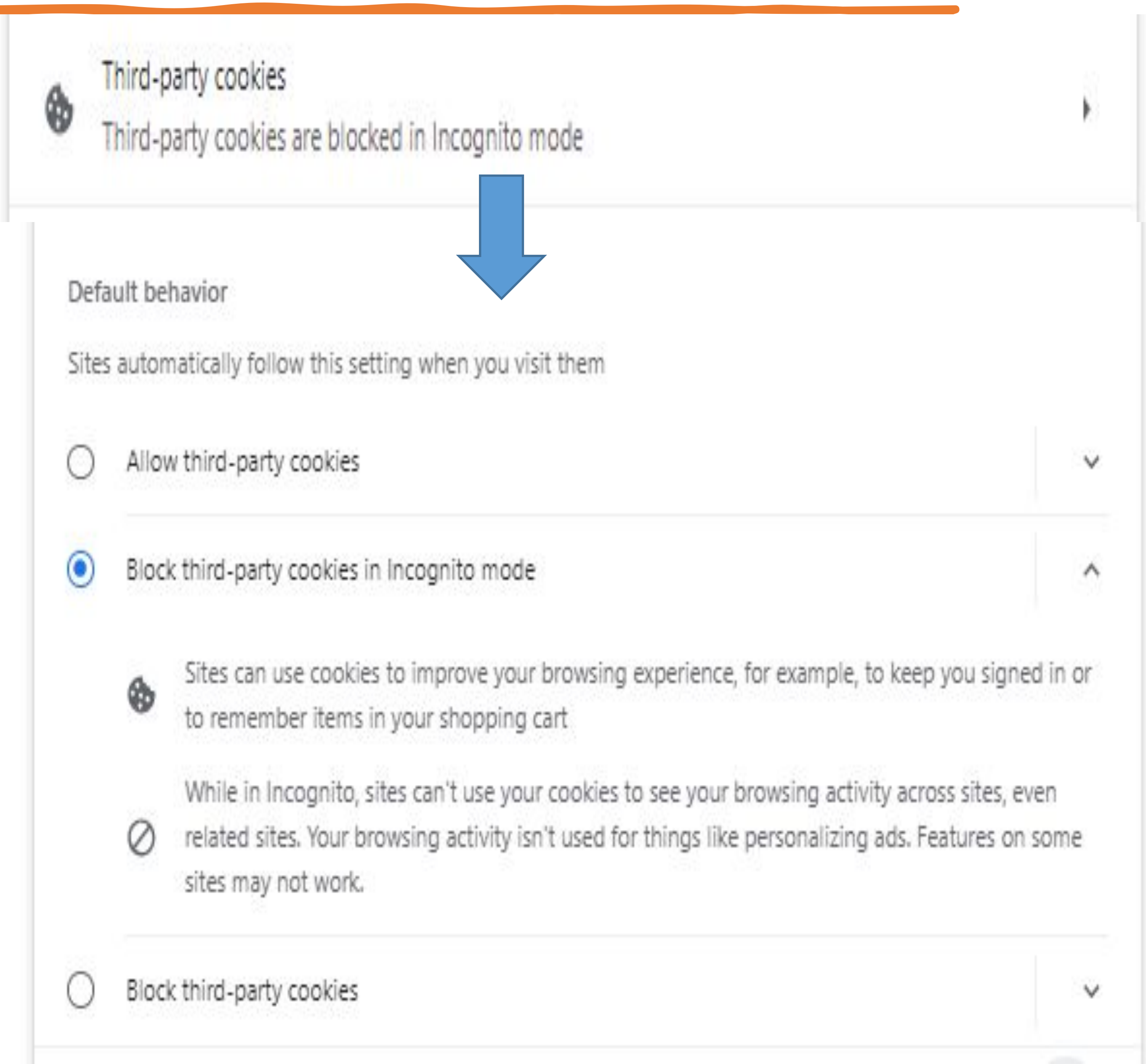
Ad privacy
Customize the info used by sites to show you ads

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site settings
Controls what information sites can use and show (location, camera, pop-ups, and more)

Browser Security : Clearing Cookies

- These are small data files stored in browser.
- Websites use cookies in order to remember **browsing history and to track user behavior on their site.**
- First party cookies are placed by the site you visit, for instance you get a first party cookie by cnn.com while visiting cnn.com.
- Third party cookies are placed by other sites, for example you get a cookie from amazon.com while visiting cnn.com.



Third-party cookies

Third-party cookies are blocked in Incognito mode

Default behavior

Sites automatically follow this setting when you visit them

○ Allow third-party cookies

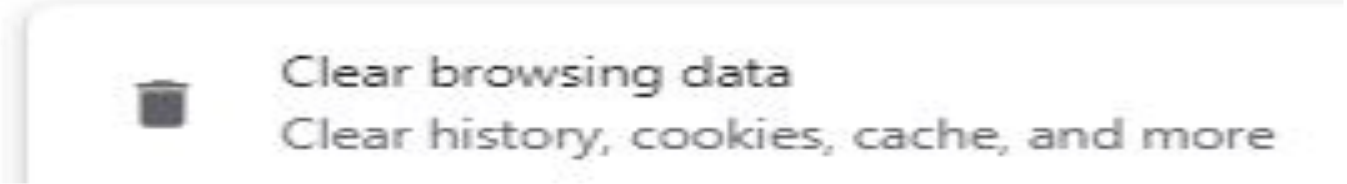
● Block third-party cookies in Incognito mode

Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart

While in Incognito, sites can't use your cookies to see your browsing activity across sites, even related sites. Your browsing activity isn't used for things like personalizing ads. Features on some sites may not work.

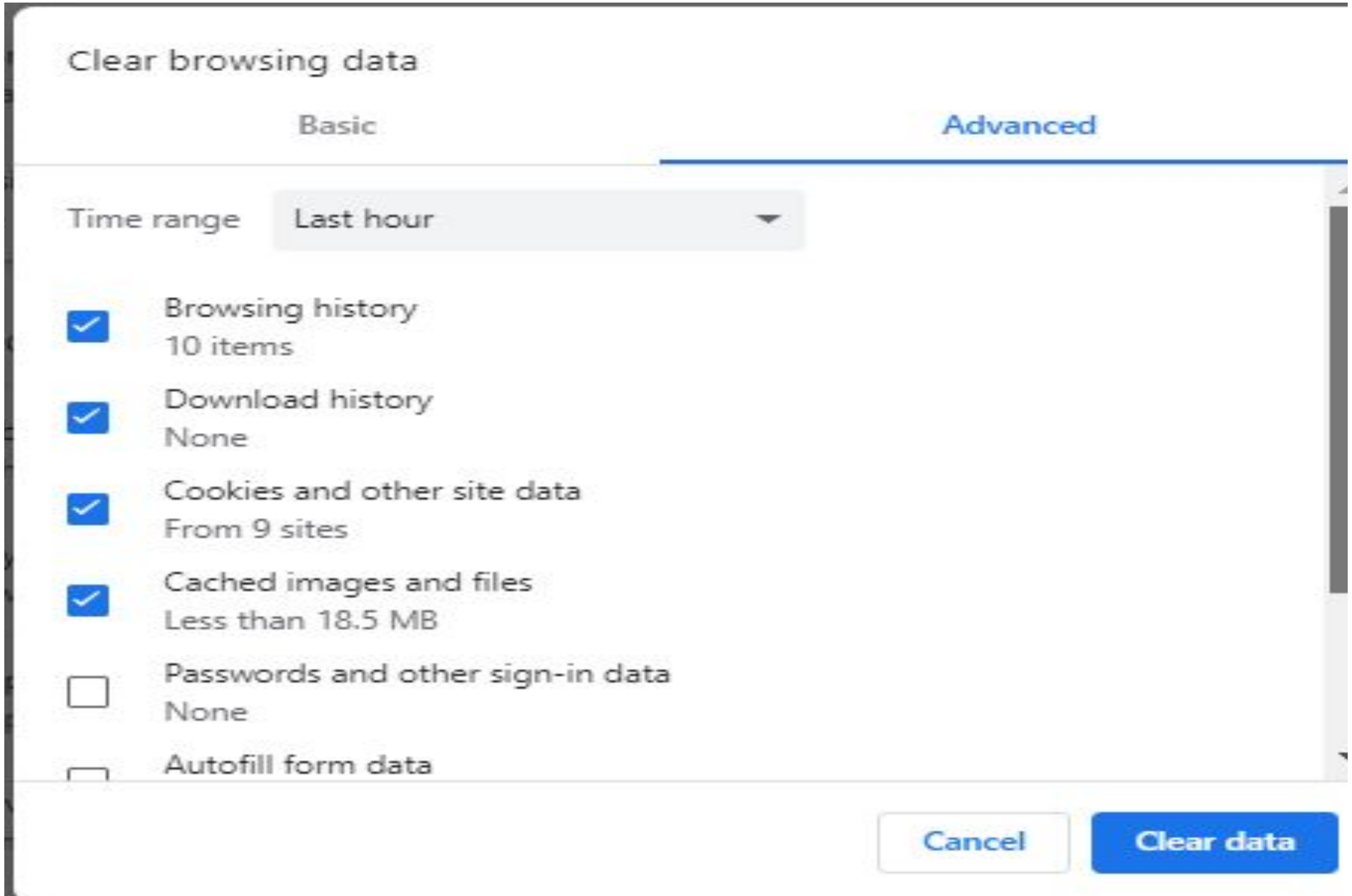
○ Block third-party cookies

Browser Security : Clearing History



Clear browsing data

Clear history, cookies, cache, and more



Clear browsing data

Time range: Last hour

☑ Browsing history
10 items

☑ Download history
None

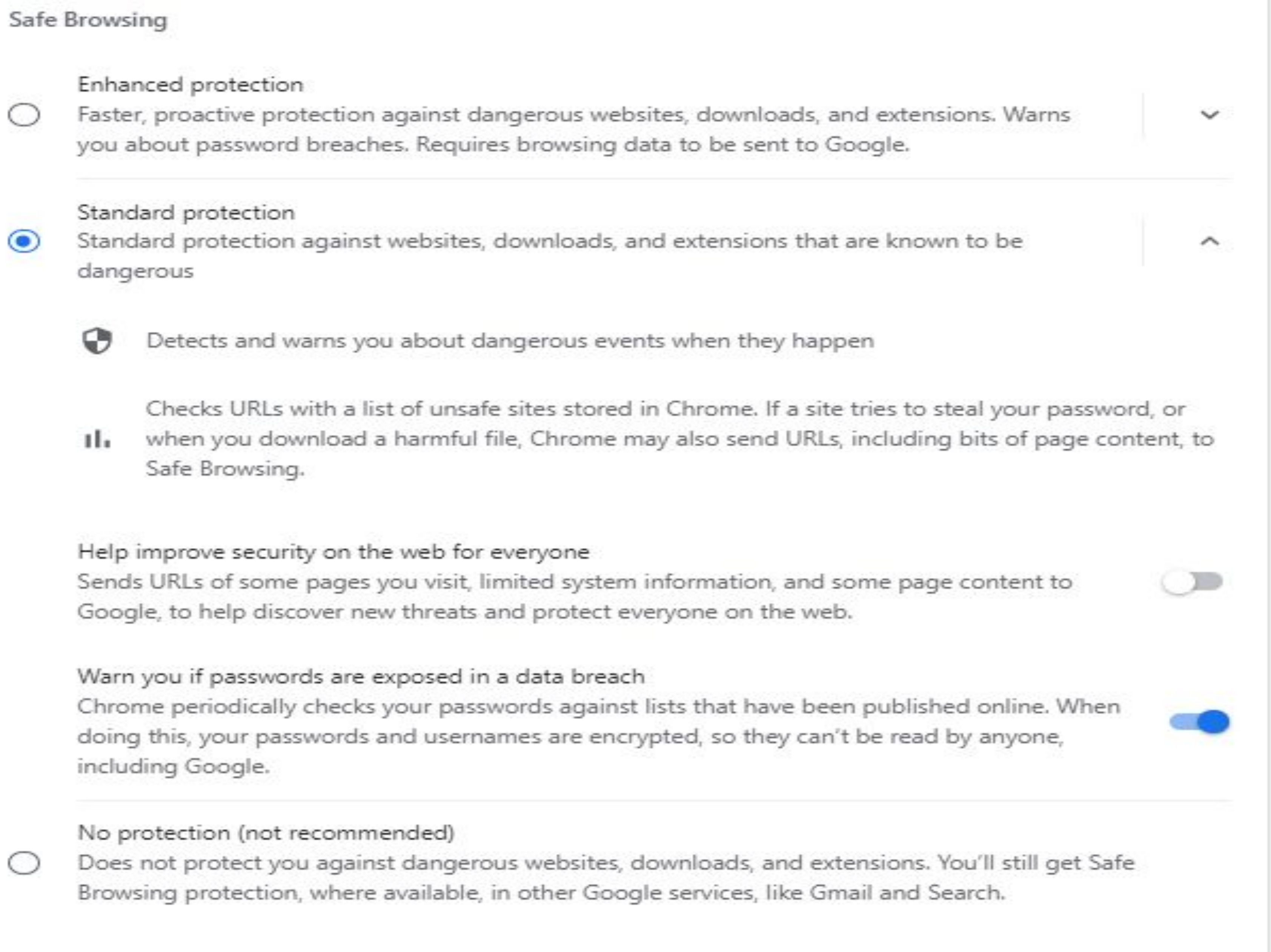
☑ Cookies and other site data
From 9 sites

☑ Cached images and files
Less than 18.5 MB

□ Passwords and other sign-in data
None

□ Autofill form data

Browser Security : Safe Browsing



Safe Browsing

○ Enhanced protection
Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

● Standard protection
Standard protection against websites, downloads, and extensions that are known to be dangerous

Detects and warns you about dangerous events when they happen

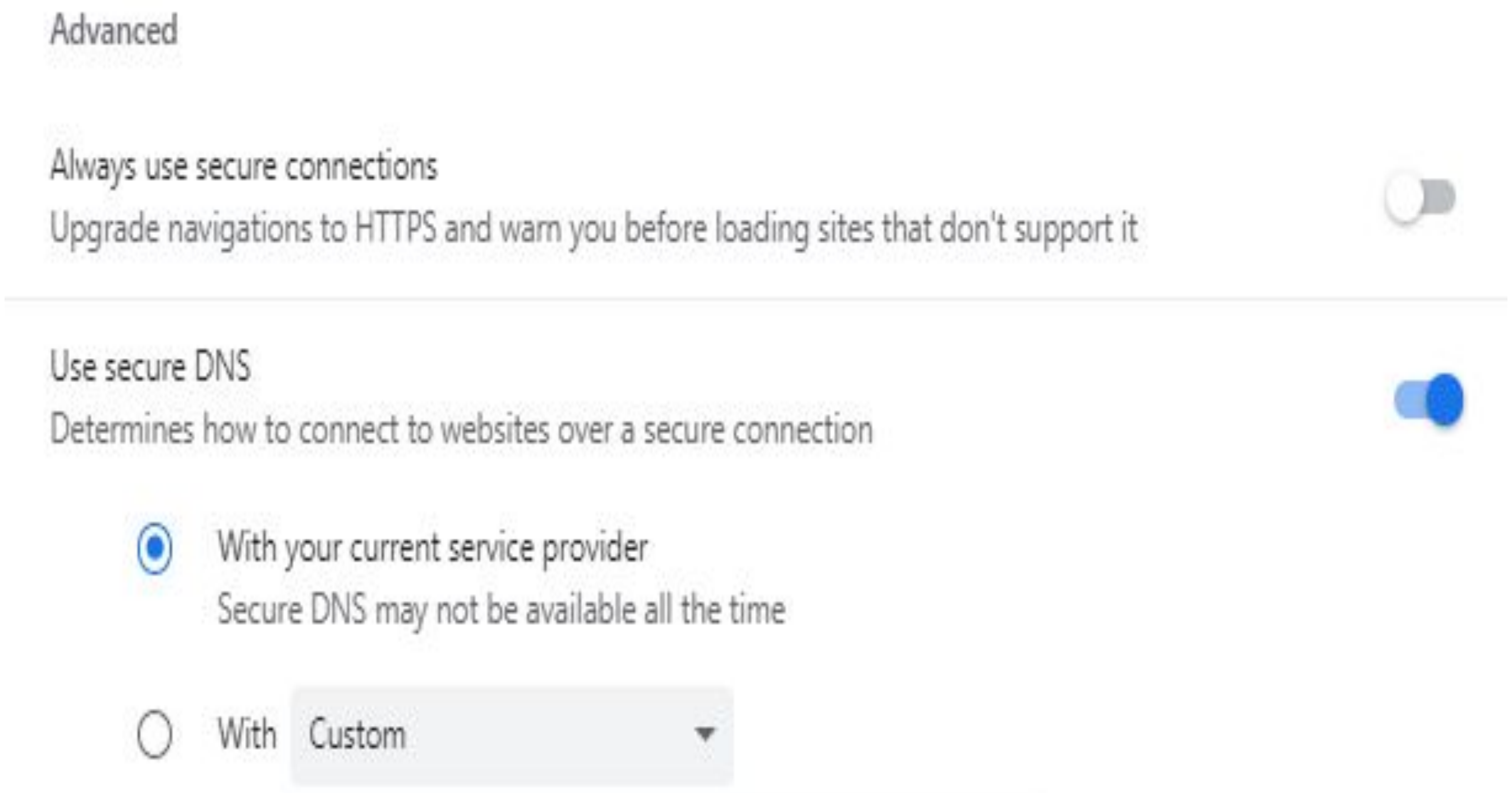
Checks URLs with a list of unsafe sites stored in Chrome. If a site tries to steal your password, or when you download a harmful file, Chrome may also send URLs, including bits of page content, to Safe Browsing.

Help improve security on the web for everyone
Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.

Warn you if passwords are exposed in a data breach
Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

○ No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Browser Security : HTTPS AND Secure DNS



Advanced

Always use secure connections

Upgrade navigations to HTTPS and warn you before loading sites that don't support it

Use secure DNS

Determines how to connect to websites over a secure connection

● With your current service provider

Secure DNS may not be available all the time

○ With Custom ▾

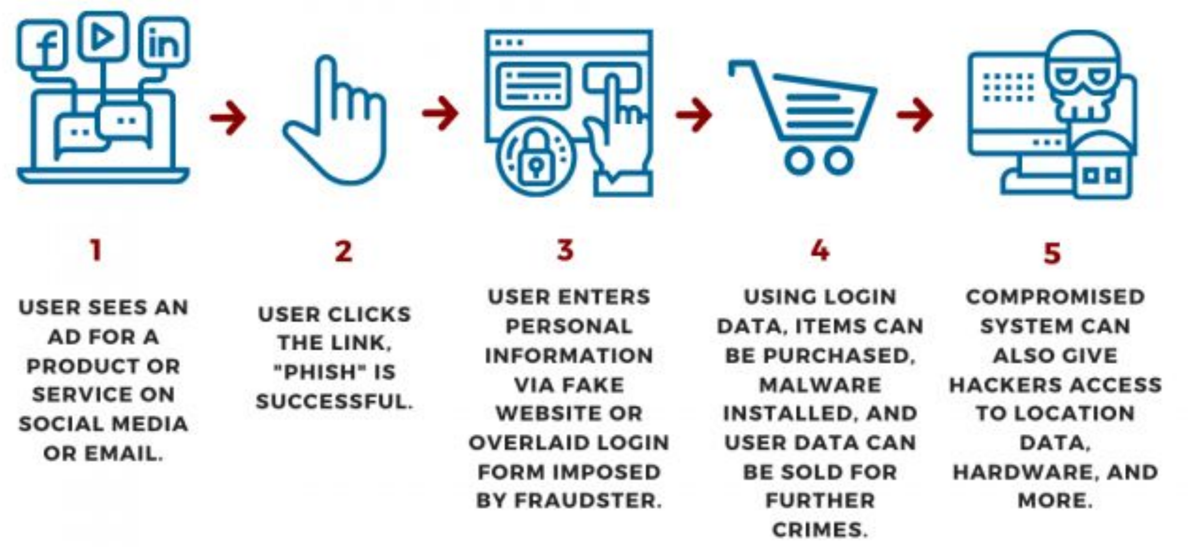
Safe Browsing

- Ensure that your operating system and key system components such as the web browser is fully patched and up to date.
- Don’t save your password in Browser.
- Install Ad block plugin or extension in your Browser to avoid adware malware.
- Avoid clicking ads, especially on popups that instruct users to download software to view content.
- Use Private/ Incognito with single tab for Financial Transaction.

Clickjacking

- Malicious technique of tricking a user of a website into performing things they are not aware of by hiding hyperlinks beneath material that is actually clickable.

- Attacker is sending users to another website that is probably controlled by a different application, domain, or both.



1 USER SEES AN AD FOR A PRODUCT OR SERVICE ON SOCIAL MEDIA OR EMAIL.

2 USER CLICKS THE LINK, "PHISH" IS SUCCESSFUL.

3 USER ENTERS PERSONAL INFORMATION VIA FAKE WEBSITE OR OVERLAID LOGIN FORM IMPOSED BY FRAUDSTER.

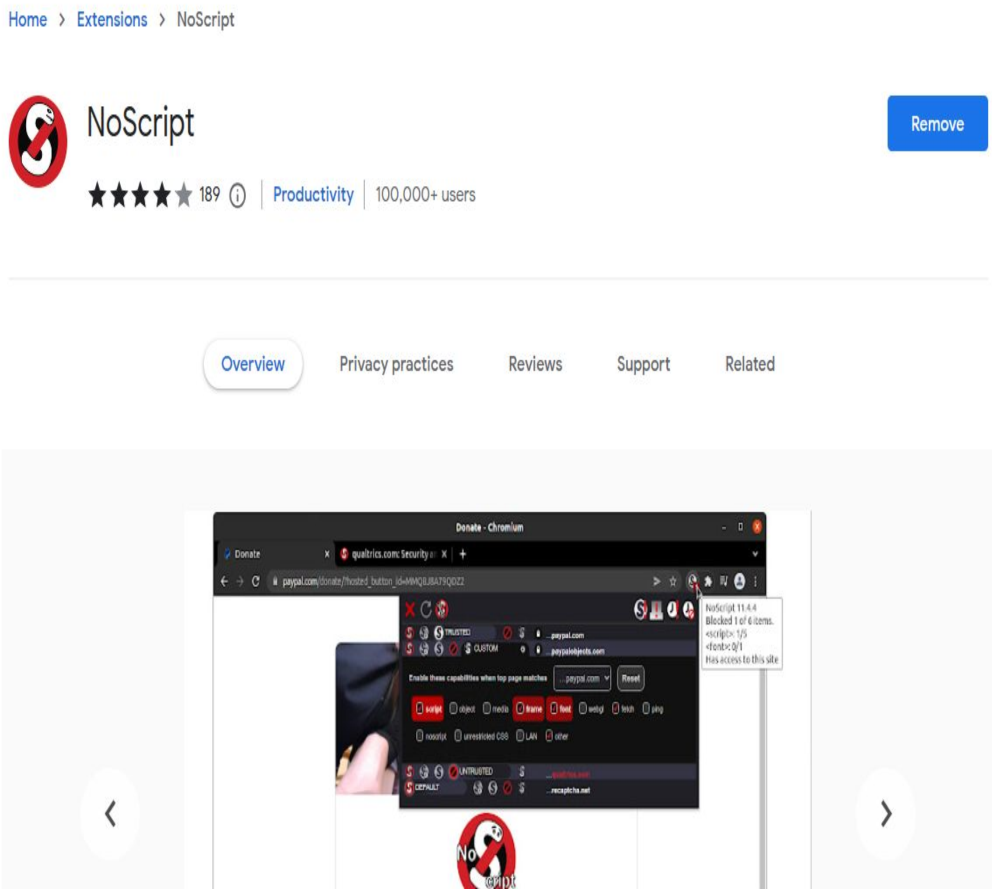
4 USING LOGIN DATA, ITEMS CAN BE PURCHASED, MALWARE INSTALLED, AND USER DATA CAN BE SOLD FOR FURTHER CRIMES.

5 COMPROMISED SYSTEM CAN ALSO GIVE HACKERS ACCESS TO LOCATION DATA, HARDWARE, AND MORE.

Image Ref: https://fraud.net/d/clickjacking//

Safeguard against Clickjacking

- keep web browsers updated & same goes for installed plugins & apps that need them, particularly Flash and Java.
- NoScript Addon in browser is highly recommended. This feature guards against great majority of types of clickjacking assaults.
- Any website that asks user to click a link to download full version of some graphic material (such films or free songs or any objectionable photgraph) or urges one to click a button to win an iPhone is probably a fraud.



Protecting Oneself when using Social Networks

- Read privacy policies published by Social Networking Service Provider & assess risks before use.
- Set online profile to private & avoid default security & privacy settings, which usually allow anyone to see user profile & post.
- Inspect privacy & security settings on social networking sites periodically.
- Inspect privacy & security settings after install or update instant messaging application.
- Adopt additional security measures such as enabling multi-factor authentication and login notification, if available.

Protecting Oneself when using Social Networks--2

- Use a different password for each of online accounts, in particular those involving sensitive information.
- Limit personal information posts including full name, address, date of birth, identity number, telephone number, credit card number, daily life schedule, etc.
- block / ignore unwanted people that you do not trust.
- Do not reply to any suspicious messages, in particular those fraudulent messages purporting to be issued from password recovery services.
- If someone asks to make financial or property transactions, check & verify authenticity of sender's identity & requested transaction.
- Check account regularly to identify any suspicious activity

Protecting Sensitive information and Online

- Use a trusted secured computer/ mobile device
- Keep softwares up-to-date (web browser, anti-malware software & firewall.)
- Protect online user account with a strong & frequently changed password.
- Always log out website or system after use & clear browser cache.
- Verify all recipient(s) of your message before send.
- Avoid sending personal or sensitive information. If necessary, encrypt information during data transmission.
- Do not respond to any suspicious email or pop-up message which asks for financial or other personal information.
- Do not disseminate or share message that contains malicious links.
- Use official mobile application to access social networking on mobile devices.

Remote Access Scam/Tech Support Scam

- Remote access scams typically entail coercing victims into granting remote access to their computers under false pretenses, such as supporting a financial transaction or "securing" their accounts.
- Once they have access to victim's computer may commit various financial frauds or outright steal money.
- Scammers will ask user to install remote access tool like Anydesk or Microsft RDP.
- After Installation they will ask for giving them permission to accept the remote access of user's system.
- They take full control of your system by changing Configuration.

Ref : https://anydesk.com/en/abuse-prevention

Protection against Remote Access Fraud

- Confirm identity: Be extremely wary if one receive’s a call or message from an unknown party requesting remote access to computer.
- Only download software for remote access from reliable sources. Verify the URL to ensure that one is on an authentic & secure website.
- Multi-factor authentication (MFA): Whenever it's feasible, turn on multi-factor authentication for your accounts.
- Neve ever reveal any passwords or remote access codes over phone or online.
- Create Awareness' by talking to your friends and family about the dangers and self-defense techniques.

Social Media Security Best Practices

- Personalizing privacy settings
- Pause before posting
- Turning off geolocation
- Using a private internet connection
- Reporting harassment or inappropriate content
- Be aware of phishing and scams
- Be aware of third-party apps and permissions
- Practice secure browsing habits
- Know how to report, block, and filter content
- Look before clicking

Cyber Laws

When the Internet was first invented, its founders barely imagined that it would grow into an all-encompassing revolution that needed to be regulated because it could be abused for illegal purposes.

There are a lot of unsettling things occurring in online these days.

The anonymity of the Internet makes it feasible to partake in a wide range of illegal acts.

People with intelligence have been egregiously abusing this feature of the Internet to continue illegal activity in cyberspace.

Indian IT ACT 2000

- The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000.
- This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations.
- It is the most important law in India dealing with Cybercrime and E-Commerce.
- The IT Act has 13 chapters and 90 sections.

Salient features of the IT Act 2000

- Digital signature has been replaced with electronic signature to make it more technology neutral act.
- elaborates on offenses, penalties, and breaches.
- outlines the Justice Dispensation Systems for cyber-crimes.
- that cyber café is any facility from where access to e internet is offered by any person in the ordinary course of business to members of the public.
- provides for the constitution of the Cyber Regulations Advisory Committee.
- based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- adds a provision to Section 81, which states that provisions of Act shall have overriding effect. It states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Amendment to Indian IT ACT 2000--- The IT Amendment Act 2008

- In IT Act 2000, there were some omissions & non-clarities in law, that resulted in investigation agency relying more & more on the time-tested (one and half century-old) Indian Penal Code.

- need for an amendment was required for I.T. Act.

- Major industry bodies were consulted & advisory groups were formed to go into perceived lacunae in the I.T. Act & comparing it with similar legislations in other nations & to suggest recommendations.

- recommendations were analysed & subsequently taken up as a comprehensive Amendment Act & after considerable administrative procedures, consolidated amendment called Information Technology Amendment Act 2008 was placed in Parliament & passed at end of 2008.

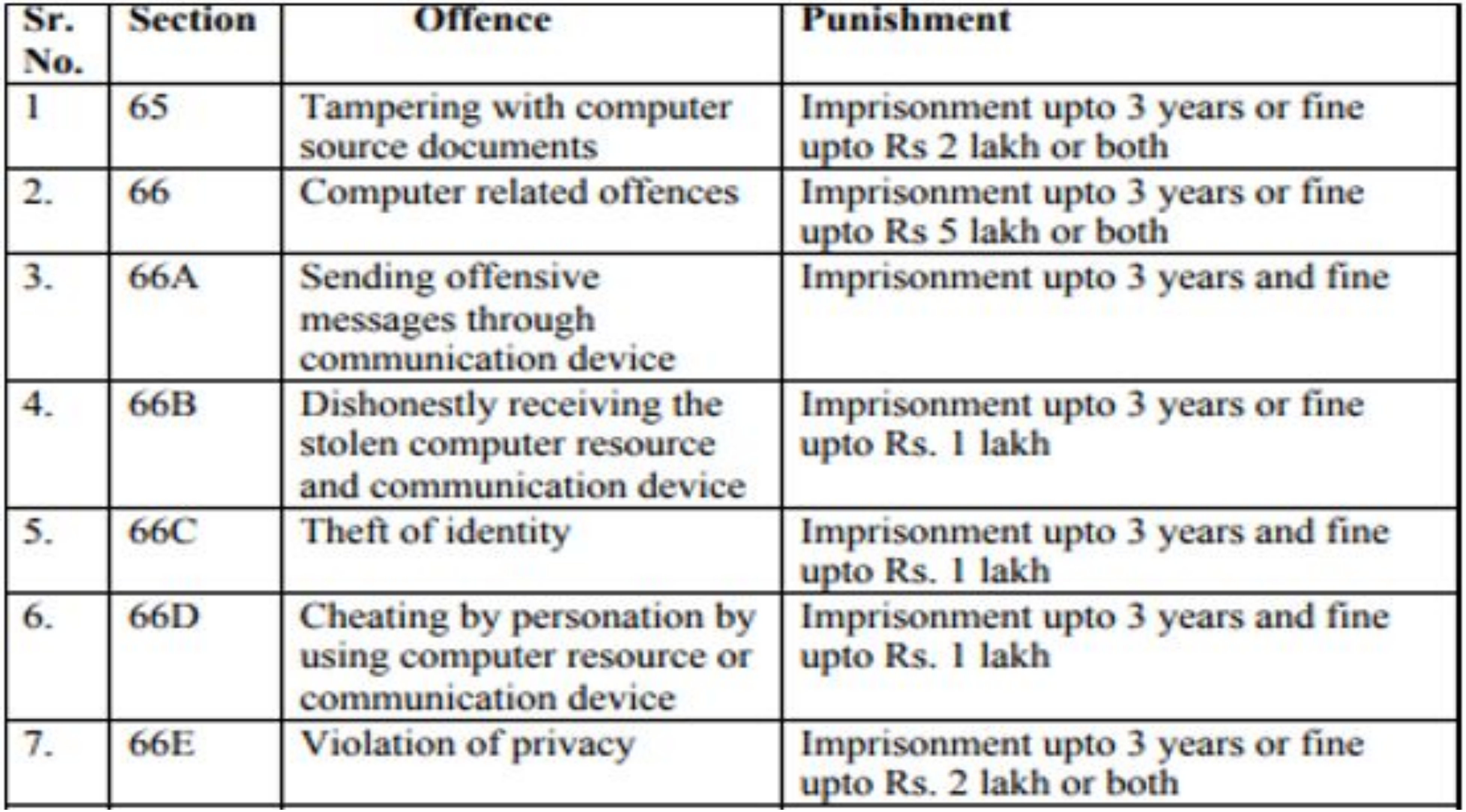
- The IT Amendment Act 2008 got the President’s approval on 5 Feb 2009 and was made effective from 27 October 2009.

The IT Amendment Act 2008

Notable features :

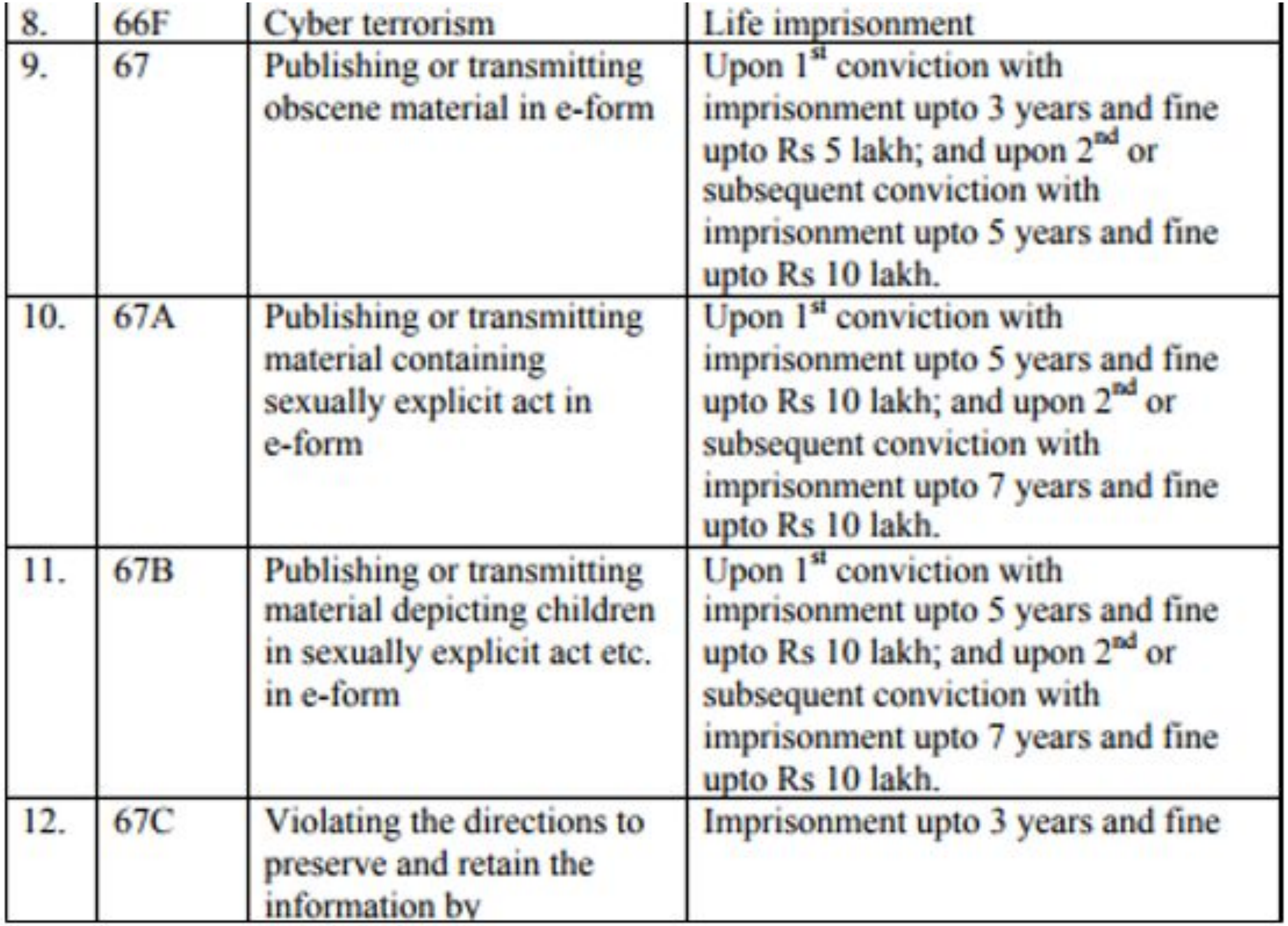
- Focusing on data privacy
- Focusing on Information Security
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyberterrorism
- Authorizing an Inspector to investigate cyber offences

A Snapshot of few Sections IT Amendment Act 2008



Sr. No.	Section	Offence	Punishment
1	65	Tampering with computer source documents	Imprisonment upto 3 years or fine upto Rs 2 lakh or both
2.	66	Computer related offences	Imprisonment upto 3 years or fine upto Rs 5 lakh or both
3.	66A	Sending offensive messages through communication device	Imprisonment upto 3 years and fine
4.	66B	Dishonestly receiving the stolen computer resource and communication device	Imprisonment upto 3 years or fine upto Rs. 1 lakh
5.	66C	Theft of identity	Imprisonment upto 3 years and fine upto Rs. 1 lakh
6.	66D	Cheating by personation by using computer resource or communication device	Imprisonment upto 3 years and fine upto Rs. 1 lakh
7.	66E	Violation of privacy	Imprisonment upto 3 years or fine upto Rs. 2 lakh or both

A Snapshot of few Sections IT Amendment Act 2008-2



8.	66F	Cyber terrorism	Life imprisonment
9.	67	Publishing or transmitting obscene material in e-form	Upon 1st conviction with imprisonment upto 3 years and fine upto Rs 5 lakh; and upon 2nd or subsequent conviction with imprisonment upto 5 years and fine upto Rs 10 lakh.
10.	67A	Publishing or transmitting material containing sexually explicit act in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
11.	67B	Publishing or transmitting material depicting children in sexually explicit act etc. in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
12.	67C	Violating the directions to preserve and retain the information by	Imprisonment upto 3 years and fine

Today’s (आज का) Cyber Security Slogan (नारा)

एडवेयर (Adware), स्पाइवेयर (Spyware), स्केयरवेयर (Scareware) सभ हेकरस (hackers) के हथकंडे हैं, मत क्लिक (Click) करो किसी भी हाइपरलिंक (Hyperlink) पे हम सभ समझदार बंदे हैं

Thank YOU all .

आप सबका बहुत आभार