spiderlink

Safe Internet Awareness Program

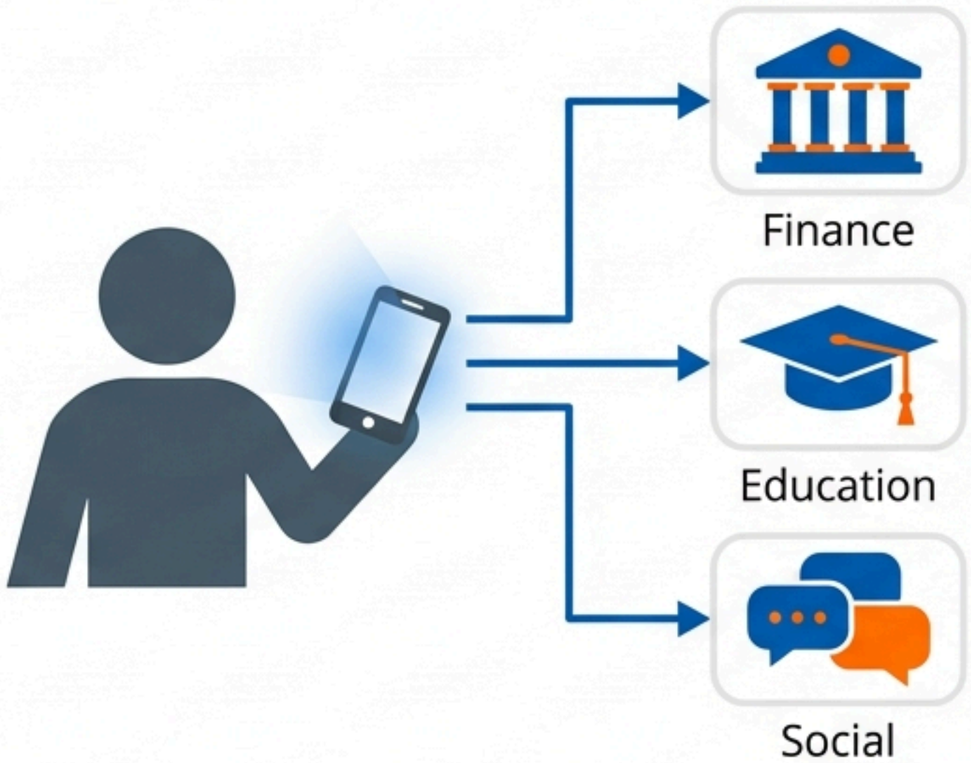
Powered by Spiderlink Networks Pvt. Ltd.

Surakshit Internet, Surakshit Jeevan

(Safe Internet, Safe Life)

A Community Initiative for Rajasthan

Why Internet Safety is Important



- The internet is integral to daily life: **Banking**, **Education**, and **Social connection**.
- Online **frauds** and **cybercrimes** are rising globally.
- **Personal data** (photos, ID) is as **valuable** as money.
- **One click** can **compromise** your finances and reputation.
- **Safety is** not technical; it is a **behavioral habit**.

REAL-LIFE SCENARIO

Imagine leaving your house door **wide open** while you sleep. Using the internet without safety precautions is exactly the **same risk**.

spiderlink

Golden Rules of Safe Internet

Protect Passwords

Never Share OTPs

Think Before Clicking

Verify Strangers

Keep Info Private

- Never share **OTPs** (One Time Passwords) or **banking PINs** with anyone.
- Use **complex, strong passwords** for all accounts.
- **Think twice** before clicking on **unknown links** (SMS/Email).
- Do not **trust messages** from unknown numbers blindly.
- **Keep personal information** (Address, DOB) private.

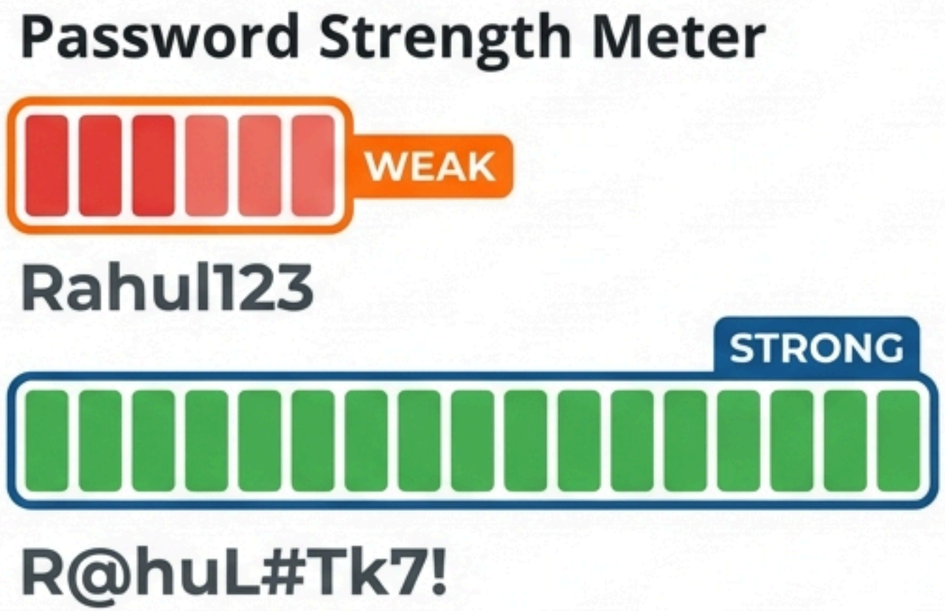
THE KEY ANALOGY

A stranger on the street asks for your house keys. You would say no. Apply the same rule when a website asks for your password.

spiderlink

Password Safety

- **Minimum length:** 8–12 characters.
- **Complexity:** Mix Upper case, Lower case, Numbers & Symbols (@#$).
- **Uniqueness:** Never use the same password for Banking and Social Media.
- **Secrecy:** Do not write passwords on sticky notes or share them.
- **Maintenance:** Change your banking passwords every 3 months.



Real-Life Example

CRACKING TIME

Weak: 'Rahul123' (Guessed in seconds). **Strong:** 'R@huL#Tk7!' (Takes centuries to crack).

Social Media Safety

- Set your profile to **'Private'** mode (Friends only).
- **Do not accept friend requests** from strangers.
- **Avoid oversharing sensitive photos** (e.g., car license plates, school uniforms).
- **Turn off 'Live Location'** sharing in posts.
- Immediately **block** and **report** suspicious or abusive profiles.

Real-Life Example

BURGLARY RISK

Posting '**Home alone for the weekend!**' tells burglars exactly when your house is empty. Post vacation photos after you return.

Common Online Frauds

Lottery Scams: Messages saying you won money without participating.

Job Scams: Offers asking for a **registration fee** before hiring.

Phishing: Fake shopping sites offering **90% discounts**.

UPI Fraud: Scammers asking you to scan a QR code to **RECEIVE** money (You only scan to **PAY**).

Fake Calls: Callers pretending to be **Bank Customer Care**.

Real-Life Example

THE LOTTERY TRAP

You receive an SMS: 'You won Rs. 1 Lakh! **Pay Rs. 2000 tax** to claim.' This is **always a fraud**. Genuine lotteries deduct tax from the winnings.

How to Identify a Scam

The Red Flags

- **Urgency:** 'Act now or your account will be **blocked!**"
- **Suspicious Links:** URLs that look wrong (e.g., amaz0n-offers.com instead of amazon.in).
- **Too Good To Be True:** Expensive smartphones selling for Rs. 2000.
- **The Ask:** Requests for **OTP**, PIN, or CVV.
- **Grammar:** Poor spelling or unprofessional language in official emails.

Real-Life Example

THE KYC SCAM

A 'Bank Manager' calls and says your KYC is expired and asks for an **OTP**. Real banks **NEVER** ask for **OTPs** over the phone.

Safe Online Shopping

- Shop only from **reputed**, **well-known** websites.
- Check for the **Padlock** icon and **'HTTPS'** in the address bar.
- **Do not save** card details on merchant websites; enter them each time.
- **Avoid** making payments while connected to **Public WiFi**.
- Enable **SMS/Email alerts** for every transaction on your bank account.
- Read **customer reviews** before buying from a new seller.

IMPOSSIBLE DEALS

A website sells branded shoes for ₹500. If the deal looks impossible, you will likely receive a fake product or a box of stones.

spiderlink

Email Safety

- Never open emails from **unknown senders**.
- Do not **download attachments** (PDF/ZIP) unless you expect them.
- **Verify** the sender's email address carefully (watch for subtle misspellings).
- **Hover over links** before clicking to see the real destination.
- **Mark suspicious emails as 'Spam'** to train your filter.

THE FAKE INVOICE

You get an email invoice for a purchase you didn't make. Clicking the attachment to 'check the error' installs a virus on your PC.

spiderlink

Mobile Phone Security

- Always use a **Screen Lock** (PIN, Pattern, Fingerprint).
- **Download apps ONLY** from **Google Play Store** or **Apple App Store**.
- Check **App Permissions:** Does a flashlight app really need access to your Contacts?
- Keep your **Operating System** (Android/iOS) **updated**.
- Install a **reputable antivirus** if using Android.

Real-Life Example

SIDE-LOADING DANGER

Downloading a 'Free Game' from a random website (APK file) often installs spyware that steals your banking SMS messages.

spiderlink

Internet Safety for Kids

- **Stranger Danger**: Never chat with people you don't know in real life.
- **Privacy**: Never share school name, home address, or phone number.
- **Openness**: Tell parents immediately if something online makes you uncomfortable.
- **Gaming**: Do not play online games with voice chat enabled with strangers.
- **Photos**: No sharing personal photos without parent permission.

Real-Life Example

THE PARK TRAP

An online 'friend' asks a child which park they play in after school. The child should immediately stop chatting and tell a parent.

spiderlink

Internet Safety for Teenagers

- **Digital Footprint**: Think before posting; the internet never forgets.
- **Bullying**: Cyberbullying is a crime; do not participate in it.
- **Respect**: Treat others online as you would face-to-face.
- **Reputation**: Offensive posts can affect college admissions or future jobs.
- **Reporting**: Report abuse or blackmail to adults immediately.

Real-Life Example

PERMANENT RECORD

Sharing an embarrassing photo of a classmate might seem funny now, but it is cyberbullying and can have legal consequences.

Online Safety for Women

- Keep social media profiles **strictly private**.
- Be cautious when accepting friend requests; **verify identity**.
- Do not share personal details (number/address) in **public comments**.
- Use **'Block'** and **'Report'** features liberally for harassment.
- **Trust your instincts**: If a conversation feels wrong, end it.

Real-Life Example

EVIDENCE GATHERING

If someone morphs your photo or threatens you online, do not delete the messages. **Take screenshots** as evidence and report to the Cyber Cell.

spiderlink

Digital Safety for Senior Citizens

- **The Golden Rule:** Banks NEVER ask for OTP or passwords over the phone.
- **Remote Access:** Never install apps like AnyDesk or TeamViewer at a caller's request.
- **Verification:** Verify payment requests with family members before proceeding.
- **Unknown Calls:** Avoid picking up calls from international or unknown numbers.
- **Confusion:** If unsure, stop and ask a younger family member.

Real-Life Example

THE ELECTRICITY BILL SCAM

A scammer claims your electricity will be cut off unless you pay Rs. 10 immediately via an app link. This is a trick to steal your entire bank balance.

spiderlink

Public WiFi Risks

- Public WiFi (Airports, Cafes, Stations) is often **unsecured**.
- Avoid accessing **Net Banking** or entering **passwords** on Public WiFi.
- Hackers can **intercept** data sent over these networks.
- Use a **VPN** (Virtual Private Network) if you must connect.
- **'Forget'** the network after you are done using it.
- Prefer using your own **Mobile Data** for sensitive tasks.

Real-Life Example

COFFEE SHOP HACK

You log into your bank account using the free WiFi at a coffee shop. A hacker sitting at the next table can intercept your login credentials.

spiderlink

Data Privacy and Protection

- **Data Minimization**: Share only what is **absolutely necessary**.
- **App Permissions**: Check what data your apps are **collecting**.
- **Terms & Conditions**: Glance through **privacy policies** before signing up.
- **Camera/Mic**: Do not allow browser access to camera/mic **blindly**.
- **Backups**: Regularly backup important data (Photos/Docs) to an **external drive**.

DATA HARVESTING

A 'Quiz App' asks for access to your contacts and gallery to tell you 'Which Celebrity You Look Like'. Deny it. It is harvesting your data.

spiderlink

Cyber Bullying Awareness

- **Cyberbullying** includes mean texts, rumors, or embarrassing photos.
- **Do Not Respond:** Bullies want a reaction; don't give it to them.
- **Block & Report:** Use platform tools to block the bully.
- **Save Evidence:** Screenshot messages before they are deleted.
- **Speak Up:** Inform parents, teachers, or authorities.
- Your **mental health** is more important than social media.

Real-Life Example

GROUP CHAT ABUSE

If you are being teased in a WhatsApp group, exit the group and report the admin. You are not obligated to stay and listen.

spiderlink

How to Report Cyber Crime in India

1930

- **National Helpline:** Dial **1930** immediately for financial fraud.
- **National Portal:** File complaints at **www.cybercrime.gov.in**.
- **Local Police:** You can also visit your nearest police station cyber cell.
- **Evidence:** Keep **screenshots**, **transaction IDs**, and **chat history** ready.
- **Timeliness:** Reporting financial fraud within the **'Golden Hour'** increases chances of recovering money.

THE GOLDEN HOUR

If money is deducted from your account due to fraud, call 1930 immediately. The police can freeze the money in the scammer's account before they withdraw it.

Your Digital Footprint

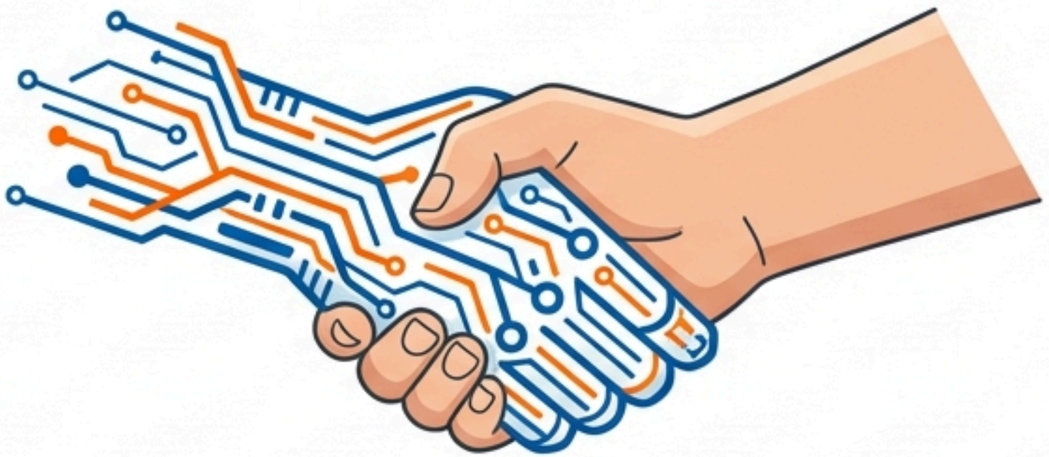
- Everything you do online leaves a **permanent trace**.
- Employers and colleges often check **social** media profiles.
- **Negative** or offensive posts can **damage** your future career.
- Think **long-term**: Will this post make me look bad in 5 years?
- Be a responsible **Digital Citizen**.

Real-Life Example

BACKGROUND CHECKS

A candidate was rejected for a job because the company found abusive language on their Twitter timeline from 3 years ago.

Spiderlink Message & Conclusion



- The Internet is a powerful tool for **learning and growth**.
- **Safety** is a shared responsibility—yours and ours.
- **Awareness** is your best **antivirus**.
- **Share this knowledge** with your family and friends.

Surakshit Internet, Surakshit Jeevan.