Contents at a glance

1. Password Threats 1
2. E-Mail Security 5
3. Online Scams 9
4. Social Networking Risks 13
5. ATM Threats 17
6. Online Banking 19
7. Online Shopping 23
8. Mobile Security 25

এক নজরে বিষয়সূচি

১. পাসওয়ার্ড থেকে বিপদ ২

২. ই-মেলের নিরাপত্তা ৬

৩. অনলাইন প্রতারণা ১০

৪. সোসাল নেটওয়ার্কিং-এর ঝুঁকি ১৪

৫. এ টি এম- এর বিপদ-আপদ ১৮

৬. অনলাইন ব্যাঙ্কিং ২০

৭. অনলাইন কেনাকাটা ২৪

৮. মোবাইল নিরাপত্তা ২৬

How to remain Cyber-safe

Here, we shall discuss eight technology-driven situations in Cyber-space and how to remain cyber-safe. Every citizen, while working with internet using computing or cell phone – should know the basics of these situations and take appropriate precautions – while working on-line. Please remember proper "awareness" and "alertness" can save you from getting into trouble in this e-world.

1. PASSWORD THREATS

The passwords should not be shared with other persons as they might be misused. The Stolen passwords can be used by unauthorized users who may collect your personal information.

Shoulder Surfing:

One way of stealing the password is standing behind an individual and note the password while he/she is typing it (Shoulder Surfing). Shoulder surfing is a direct observation technique to get passwords, PINs, other sensitive personal information one may listen in on your conversation if you give your credit-card number over the phone. Shoulder surfing is easily done in crowded places. It's comparatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine. or use a calling card at a public pay phone. Do not write passwords in disk or paper so that the Cheater get it easily.

Bruteforce attacks:

Another way of stealing the password is through guess. Hackers try all the possible combinations with the help of personal information of an individual. They will try with the person's name, pet name (nick name), numbers (date of birth, phone numbers), school name ... etc. When there are large number of combinations of passwords the hackers uses fast processors and some software tools to crack the password. This method of cracking password is known as "Brute force attack".

সাইবার নিরাপত্তা কোন পথে ?

এখানে আমরা তথ্যপ্রযুক্তিজনিত আটটি বিষয়ের আলোচনা করব যা থেকে আমরা বোঝার চেষ্টা করব কেমনভাবে আমাদের ব্যক্তিগত তথ্য নিরাপদ ও সুরক্ষিত রাখা যাবে। **কম্পিউটার** ও মোবাইলের মাধ্যমে সকল ইন্টারনেট ব্যবহারকারীর ইন্টারনেট ব্যবহার করার আগে প্রাথমিক কিছু জ্ঞান থাকা আবশ্যক; যে জ্ঞান তাদের প্রয়োজনীয় রক্ষাকবচের কাজ করবে। মনে রাখবেন, সঠিক সচেতনতা ও সঠিক সতর্কতা আজকের ই-বিশ্বের অবাঞ্ছিত হয়রানি থেকে আপনাকে মুক্ত রাখবে।

১. পাসওয়ার্ড থেকে বিপদ (Password Threats)

আপনার পাসওয়ার্ড অন্য কাউকে জানাবেন না। পাসওয়ার্ড চুরিও হতে পারে। এরকম হলে তার অপব্যবহার হতে পারে এবং আপনার ব্যক্তিগত তথ্য অন্যকেউ জেনে ফেললে আপনি বিপদে পড়তে পারেন।

উঁকি-ঝুঁকি মারা (Shoulder Surfing)

উঁকি-ঝুঁকি মারা বা সোল্ডার সার্ফিং একরকম পাসওয়ার্ড চুরির পদ্ধতি। আপনি যখন আপনার **কম্পিউটার** বা মোবাইলে আপনার পাসওয়ার্ড বা পিন নম্বর টাইপ করেন তখন অনেক সময় কেউ পিছন থেকে বা আড়ালে দাঁড়িয়ে তা দেখে ফেলতে পারে বা চুরি করতে পারে। এ টি এম-এ টাকা তোলার সময় বা ফোনে আপনি যখন কাউকে আপনার ডেবিট/ক্রেডিট কার্ডের নম্বর বলছেন— এমন সময় একজন প্রতারক তা সহজেই দেখে বা শুনে ফেলতে পারে, যার ফলে আপনি সর্বস্ব খোয়াতে পারেন। **কম্পিউটার**রের হার্ডডিস্ক বা অন্যকোথাও আপনার পাসওয়ার্ড লিখে রাখবেন না যাতে করে প্রতারক সহজেই তা জেনে যেতে পারে।

গা-জোয়ারি আক্রমণ (Bruteforce attacks)

পাসওয়ার্ড চুরি করার অন্য একটা পদ্ধতি হল অনুমানের উপর নির্ভর করা। আপনার নাম, ডাকনাম, জন্মতারিখ, স্কুলের নাম ইত্যাদি জেনে নিয়ে হ্যাকাররা বিশেষ সফটওয়্যার বা টুলের সাহায্যে আপনারপাসওয়ার্ড ভেঙে ফেলতে পারে। এই পদ্ধতিই ব্রুটফোর্স অ্যাটাক (Bruteforce attack) বা গা-জোয়ারি আক্রমণ নামে পরিচিত।

Dictionary attacks:

Hackers also try with all possible dictionary words to crack your password with the help of some software tools. This is called a "Dictionary attack".

Sharing your passwords with strangers:

Sharing the passwords with the unknown persons (strangers) may also lead to loss of your personal information. They can use your login information and can get the access to your information. The operating system does not know who is logging into the system, it will just allow any person who enters the credential information into the login page. The persons like strangers after getting access to your information they can do anything with it. They can copy, modify or delete it.

Guidelines for maintaining a good password

- Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc.
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Do not use the name of things located around you as passwords for your account.
- Be aware of Shoulder Surfers at public places or schools while entering your passwords. Cover the keyboard with paper or hand or something else from viewed by unauthorized users.
- You should not write the passwords on the paper or on any disk drive to store it, brain is the best place to store them.
- You should not use a password that represents their personal information like nicknames, phone numbers, date of birth etc.

অভিধান আক্রমণ (Dictionary attacks)

''হ্যাকার'' নামক বিশেষরকম দক্ষ ব্যক্তিরা বিশেষ সফটওয়্যার ও টুলের সাহায্যে অভিধানের সম্ভাব্য সব শব্দ ব্যবহার করে আপনার পাসওয়ার্ড ভেঙে ফেলতে পারে— এই পদ্ধতিকে বলে ডিকশনারি অ্যাটাক।

অচেনা অজানা ব্যক্তির সঙ্গে আপনার পাসওয়ার্ড জানা-জানি করলে আপনি বিপদে পড়তে পারেন; আপনার ব্যক্তিগত তথ্য বেহাত হতে পারে। এমন হলে তারা আপনার সিস্টেমে ঢুকে পড়ে তা ব্যবহার করতে পারে। ঐ সময় আপনি না আর কেউ আপনার সিস্টেমে ঢুকে রয়েছে তা আপনার সিস্টেম জানতে পারবে না। হ্যাকাররা এইভাবে ঢুকে পড়ে আপনার তথ্য কপি করতে, পাল্টাতে বা মুছে দিতে পারে।

নিরাপদ পাসওয়ার্ডের জন্য পরামর্শ

●আট বা তার বেশি অক্ষরের পাসওয়ার্ড ব্যবহার করুন। পাসওয়ার্ড বেশি অক্ষরের হলে আপনার সুরক্ষাও শক্তিশালী হবে।
●পাসওয়ার্ড তৈরির সময় অক্ষরের সঙ্গে সংখ্যা ও বিশেষ ক্যারেকটার ও চিহ্ন ব্যবহার করুন।
●অভিধান থেকে শব্দ নিয়ে তা পাসওয়ার্ড হিসেবে ব্যবহার করবেন না; এরকম পাসওয়ার্ড সহজেই বের করে ফেলা যায়।
●এমন পাসওয়ার্ড ব্যবহার করবেন যা কোথাও লিখে রাখার দরকার পড়ে না, সহজেই মনে রাখা যায়।
●পাসওয়ার্ড যেন হ্যাকাররা সহজে অনুমান করতে না পারে, এটা খেয়ালে রাখুন।
●আপনার পাসওয়ার্ড কেউ জেনে ফেলেছে সন্দেহ হলে শীঘ্র পাল্টে নিন ; পনের দিন অন্তর পাসওয়ার্ড বদল করুন।
● আগে ব্যবহার করা কোনো পাসওয়ার্ড পুনরায় ব্যবহার করবেন না।
●আপনার আশেপাশে কেউ থাকলে পাসওয়ার্ড ব্যবহারের সময় সতর্ক থাকুন।
●পাসওয়ার্ড হিসেবে আপনার চারপাশে দৃশ্যমান কোনো জিনিসের নাম ব্যবহার করবেন না।
●স্কুলে বা কোনো প্রকাশ্যস্থানে (Public Place) পাসওয়ার্ড ব্যবহারের সময় সাবধান থাকুন যাতে উঁকি-ঝুঁকি মেরে কেউ তা দেখে না ফেলে। একরম সময়ে হাত বা কাগজ দিয়ে কি-বোর্ড যথাসম্ভব আড়াল করুন।
●পাসওয়ার্ড কোথাও লিখে রাখবেন না, আপনার ''মাথা''-ই হল আপনার পাসওয়ার্ড সুরক্ষিত থাকার উপযুক্ত স্থান।
●আপনার নাম, ডাকনাম, জন্মতারিখ, স্কুলের নাম ইত্যাদি পাসওয়ার্ড হিসেবে ব্যবহার করবেন না।

2. E-MAIL SECURITY

E-mails are just like postcards from which the information can be viewed by anyone. When a mail is transferred from one mail server to another mail server there are various stops at which there is a possibility of unauthorized users trying to view the information or modify it.

Since a backup is maintained for an e-mail server, all the messages will be stored in the form of clear text though they have been deleted from your mailbox. Hence, there is a chance of viewing the information by the people who are maintaining backups. So, it is not advisable to send personal information through e-mails.

Some examples of e-mail fraud

- Say, you have won a lottery of million dollars, getting or receiving such kind of mails is a great thing, and really it's the happiest thing. However, these mails may not be true. By responding to such a kind of mails many people lost huge amount of money. So ignore such kind of e-mails, do not participate in it and consider it as a scam.

- Sometimes e-mails offering free gifts and asking personal information are received from unknown addresses. This is one way to trap your personal information.

- Generally spammers or hackers try to steal e-mail address and send malicious software or code through attachments, fake e-mails, and spam and also try to collect your personal information.

২. ই-মেলের নিরাপত্তা (E-mail Security)

ই-মেল হল একটা পোস্টকার্ডের মতো যার তথ্য অন্যরা জেনে ফেলতে পারে। যখন কোনো ই- মেল একটা সার্ভার থেকে অন্য সার্ভারে স্থানান্তরিত হয় তখন অনেকগুলি ধাপ অতিক্রম করতে হয় এবং এই ধাপগুলি অতিক্রম করার সময় অন্যব্যক্তি তা জেনে ফেলতে পারে।

আপনি আপনার মেলবক্স থেকে সব মুছে (Delete) ফেললেও মেল সার্ভারে তা ব্যাকআপ হিসেবে জমা থেকে যায়। আবার এই ব্যাকআপ যারা তত্ত্বাবধান করেন তাদের মাধ্যমে আপনার ব্যক্তিগত তথ্য অন্যদের জেনে যাবার একটা সম্ভাবনা থেকে যায়। তাই-মেলের মাধ্যমে ব্যক্তিগত তথ্য আদান-প্রদান করবেন না।

ই-মেলের মাধ্যমে প্রতারণার কয়েকটি উদাহরণ

●“আপনি লক্ষাধিক টাকার লটারি জিতেছেন”— এজাতীয় লোভনীয় ই-মেলের ফাঁদে পড়ে উত্তর দিতে গিয়ে বহু মানুষ প্রতারিত হয়েছেন। ফাঁদে পড়বেন না। এগুলিকে উপেক্ষা করুন এবং প্রতারণা হিসেবেই বিবেচনা করুন।

●অনেক সময় অজানা ঠিকানা থেকে বিনামূল্যের উপহারের লোভ দেখিয়ে ই-মেলে আপনার ব্যক্তিগত তথ্য জেনে নেওয়ার জন্য ফাঁদ পাতা হয়।

●সাধারণভাবে প্রতারকেরা ই-মেল ঠিকানা (e-mail address) চুরি করে নানা ধরনের প্রলোভন দেখিয়ে ভুয়ো মেল পাঠায়; আপনি তাতে অংশগ্রহণ করলে বিশেষ বিশেষ কৌশলে তারা আপনার ব্যক্তিগত তথ্য সংগ্রহ করে নেয়।

Guidelines for using e-mail safely

- Since the e-mail messages are transferred in clear text, it is advisable to use some encryption software like PGP (pretty good privacy) to encrypt e-mail messages before sending, so that it can be decrypted only by the specified recipient only.

- Use e-mail filtering software to avoid Spam or so unwanted mails that only messages from authorized users are received. Most e-mail providers offer filtering services.

- Do not open attachments coming from strangers, since they may contain a virus along with the received message.

- Be careful while downloading attachments from e-mails into your hard disk. Scan the attachment with updated antivirus software before saving it

- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it .

- Avoid sending personal information through e-mails.

- Avoid filling forms that come via e-mail asking for your personal information and do not click on links that come via e-mail.

- Do not click on the e-mails that you receive from unknown users.

ই-মেল নিরাপত্তার জন্য কী করবেন?

●কেবলমাত্র টেক্সট মেসেজই ই-মেলে পাঠান এবং পাঠানোর আগে গোপনীয়তা রক্ষার জন্য PGP বা Pretty Good Privacy জাতীয় সফটওয়্যার ব্যবহার করুন।

●এলোমেলো বা স্প্যাম মেল এড়ানোর জন্য ই-মেল বিশেষ ধরণের (Filter) সফটওয়্যার ব্যবহার করুন। সমস্ত ইন্টারনেট প্রদানকারী-সংস্থাই এই পরিষেবা দিয়ে থাকে। কেবলমাত্র বৈধ ব্যক্তির সঙ্গেই ই-মেল আদান-প্রদান করুন।

●সন্দেহজনক ই-মেলের সঙ্গে আসা সংযুক্তি (attachment) খুলবেন না; এগুলির মধ্যে ভাইরাস থাকতে পারে।

●ই-মেলের সঙ্গে আসা কোনো সংযুক্তি (attachment) ডাউনলোড করার সময় সতর্ক থাকতে হবে। অতি অবশ্যই সেগুলি হার্ডডিস্কে সঞ্চয় করার আগে উপযুক্ত অ্যান্টিভাইরাস চালিয়ে স্ক্যান করতে হবে— ভাইরাসকে নিষ্ক্রিয় করার জন্য।

●ই-মেলের সঙ্গে কার্যকর সংকেতযুক্ত (executable code) কোনো সংযুক্তি পাঠাবেন না; যেমন ওয়ার্ড ডকুমেন্টের সঙ্গে ম্যাক্রো (Macro), এক্সেল ফাইলের সঙ্গে জিপ ফাইল (ZIP File) ইত্যাদি। এসবের বদলে কেবলমাত্র রিচ টেক্সট ফরম্যাট ব্যবহার করলেই নিরাপদ থাকতে পারবেন। এ ব্যাপারে RTF আপনাকে সুরক্ষিত রাখতে পারে। কিন্তু এর সঙ্গে ম্যাক্রো যুক্ত করা যাবে না। যদি আপনি ইতোমধ্যেই অন্যের পাঠানো ভাইরাসে আক্রান্ত না হয়ে থাকেন তাহলে এই ব্যবস্থার দ্বারা আপনি সুরক্ষিত থাকতে পারবেন।

●ই-মেলের মাধ্যমে ব্যক্তিগত তথ্য আদান-প্রদান করা থেকে বিরত থাকুন।

●ব্যক্তিগত তথ্য দিয়ে ই-মেলের মাধ্যমে আসা ফর্ম পূরণ করবেন না। ই-মেলে আসা কোনো লিংক-এ ক্লিক করবেন না।

●অজ্ঞাত পরিচয় ব্যক্তির কাছ থেকে পাওয়া ই-মেল খুলবেন না।

3. ONLINE SCAMS

Online scam is an attempt to trap you for stealing money. There are many types of online scams, this includes stealing money with fake names, fake photos, fake e-mails, forged documents, fake job offers and many more. Generally, it happens by sending fake e-mails for your personal details like online banking details, credit card details. Sometimes e-mails are sent from lottery companies with fake notice, whenever you participate in online auction and e-mails received for fake gifts.

Phishing scam: Online scammers send you an e-mail and ask your account information or credit card details along with a link to provide your information. Generally, the links sent will be similar to your bank. So whenever you post your details in the link then the details will be received by scammers and money is misused.

Lottery scam: Sometimes you receive an e-mail like "you won a lottery of million dollars" receiving such kind of mails is a great thing, and really it's a happiest thing. By responding to such kind of mails huge amount of money will be lost. As these e-mails are not true, scammers try to fool and trap you to obtain money.

Online Auction: If you bid for a product you never get the product promised or don't match the product, and the description given to you may be incomplete, wrong, or fake. The scammer accepts the bid from one person and goes for some other sites where they can get less than the winning bid so scammers may not send the product you wanted.

Forwarding Product or Shipping Scam: Generally, it happens for products that are purchased through online advertisement. Cheating may be done using stolen credit cards and shipping to your mail address. You will be fooled and asked to reship the product to others they might have deceived, who would again reship the product overseas.

৩. অনলাইন প্রতারণা (Online Scams)

অনলাইনে আপনার অর্থ আত্মসাৎ করার জন্য বিভিন্নভাবে জাল বিস্তার করা হয়। নানাভাবে এই প্রতারণা হতে পারে, যেমন ভুয়ো নাম ও ছবি ব্যবহার করে, চাকরির মিথ্যা প্রলোভন ইত্যাদি দেখিয়ে। সাধারণত ভুয়ো ই-মেল পাঠিয়ে আপনার অনলাইন ব্যাঙ্কিং ও ডেবিট/ক্রেডিট কার্ড সংক্রান্ত তথ্য জানতে চাওয়া হয়। কখনো কখনো আপনি লটারিতে প্রচুর টাকা জিতেছেন বা মূল্যবান উপহার পেয়েছেন এমন খবর জানিয়ে আপনার কাছে ই-মেল পাঠানো হয় যাতে আপনি লোভে পড়ে ঐসমস্ত ই-মেল পড়েন এবং তাতে অংশগ্রহণ করেন।

ফিসিং স্ক্যাম (Phishing Scams)

অনলাইন প্রতারকরা ই-মেলে একটা লিংক দিয়ে আপনার ব্যাঙ্কের বিস্তারিত তথ্য জানতে চায় এবং একই লিংক তারা আপনার ব্যাঙ্কেও পাঠায়। যখনই আপনি ঐ লিংকে আপনার ব্যাঙ্কের তথ্যাবলি পাঠিয়ে দেন তখন তা চলে যায় ঐ প্রতারকদের কাছে— এইভাবে প্রতারকরা আপনার টাকা সরিয়ে ফেলতে পারে।

লটারি স্ক্যাম (Lottery Scam)

বিভিন্ন সময় "**আপনি লটারিতে লক্ষাধিক টাকা জিতেছেন**" এমন ই-মেলও পেতে পারেন। এই জাতীয় ই-মেলে প্রলুব্ধ হয়ে উত্তর দিলেই আপনার অর্থহানি ঘটতে পারে।

অনলাইন নিলাম (Online Auction)

অনলাইন নিলামে প্রতারকরা একটি জিনিস দেখিয়ে আপনার টাকা নিয়ে তার চেয়ে কম দামের আপনার দরকারি/অদরকারি জিনিস গছিয়ে দেওয়ার চেষ্টা করতে পারে। এজন্য তারা কৌশলে নানা লোভনীয় জিনিসের ছবি দেখায়, মিথ্যা ও অসম্পূর্ণ তথ্য ব্যবহার করে; ফলে আপনি আপনার চাওয়া দ্রব্যটি পেলেন না বা পেলেন কোনো স্বল্পমূল্যের দ্রব্য যা আপনি চান নি।

শিপিং স্ক্যাম (Shipping Scam)

অনলাইন বিজ্ঞাপনের মাধ্যমে চুরি করা ক্রেডিট কার্ড দিয়ে কেনা নানা মূল্যবান সামগ্রীর প্রতি আপনি আকৃষ্ট হলে আপনার ঠিকানায় তা পাঠিয়েও প্রতারণা করা হতে পারে। আমেরিকান বা কোনো বিদেশি বহুজাতিক সংস্থার নাম ব্যবহার করে এসব প্রতারণা করা হয়।

E-mail Scam: Sometimes you get an e-mail with a message like — you have won something special like digital camera, webcam - all you need to do is just visit our web site by clicking the link given below and provide in your debit or credit card details to cover shipping and managing costs. However, the item never arrives but after some days the charges will be shown on your bank account, and you will lose money.

By e-mails: Generally, fraudsters send you an e-mail with tempting offers of easy access to a large sum of money and ask you to send scanned copies of personal documents like your address proof, passport details and ask you to deposit an advance fee for a bank account. So once you deposit the funds, they take money and stop further communication, leaving you with nothing in return.

Tips to Prevent Online Scams

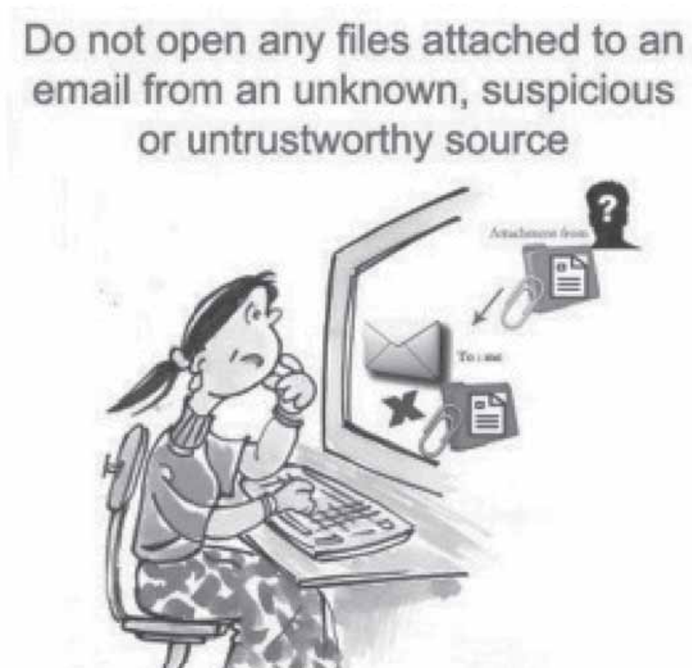
Confirm whether e-mail is received from bank or not: Be cautious while providing bank details online and before proceeding further confirm with the bank about the e-mail you received. Think that, if something is important or urgent why doesn't the bank call me instead of sending e-mail?

Confirm the shipping: Beware of shipping scam. Make sure you get authorized signed document via fax before proceeding further and make sure that you receive it from an authorized company.

Be cautious during online auction: Don't be trapped with discounts and think wisely before you proceed with online auction. Think why $200 product would be $ 20.

Be aware about the product you receive via e-mail: Be aware about the products you get for a discounted price. Think why you have received e-mail for products when you never enter any online shopping or contest.

Don't be trapped by lottery scam: Don't get trapped by scammers and e-mails with a subject line you won some $10000. Just think why only you have received the e-mail without your participation!



ই-মেল স্ক্যাম (E-mail Scams)

লটারিতে আপনি ওয়েব ক্যামেরা বা ডিজিটাল ক্যামেরা জিতেছেন বলে অভিনন্দন জানিয়ে ই-মেল আসতে পারে। এই ধরনের ই-মেলের সঙ্গে অন্য ওয়েবসাইটের লিংক দেওয়া থাকে যাতে ঢুকে পড়লে আপনার ডেবিট কার্ড ও ক্রেডিট কার্ডের বিস্তারিত তথ্য জানাতে বলা হয় ঐ দ্রব্যগুলি আপনার ঠিকানায় পাঠানোর খরচের জন্য। কিন্তু ঐ দ্রব্যগুলি কখনোই আসে না অথচ আপনার ব্যাঙ্ক অ্যাকাউন্ট থেকে টাকা কাটা যায়।

"**সহজে আয় করুন**" জাতীয় লোভনীয় বিজ্ঞাপনে আপনার শিক্ষাগত যোগ্যতা ও পরিচয়পত্রের যেমন পাসপোর্ট, অ্যাডমিট কার্ড ইত্যাদি স্ক্যান করে পাঠাতে বলা হয় এবং সঙ্গে ফি বাবদ টাকা জমা করতে অনুরোধ করা হয়। আপনি টাকা জমা দেওয়ার পর তারা পরবর্তী সময়ে আর কোনোরকম যোগাযোগ রাখে না।

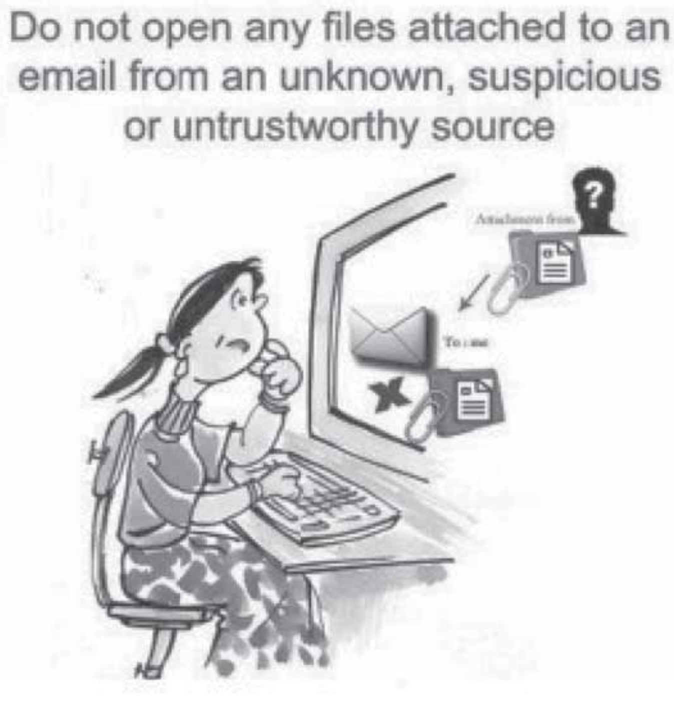
প্রতিরোধের জন্য প্রয়োজনীয় পরামর্শ

●বিস্তারিত তথ্য দেবার সময় সবার আগে আপনার ঠিকানায় আসা ই-মেলটি সত্যিই ব্যাঙ্ক থেকে এসেছে কিনা নিশ্চিত হোন। এভাবে ভাবুন— জরুরি থাকলে ব্যাঙ্ক আপনাকে ফোন করে ডেকে না পাঠিয়ে ই-মেল করল কেন?

● শিপিং স্ক্যামের বিয়য়ে ফ্যাক্স বা অন্যকোনো বৈধ উপায়ে বিষয়টি যাচাই করে তবে পরবর্তী ধাপে যান।

●অনলাইন নিলামের বিষয়ে সতর্ক থাকুন। "**বিশেষ ছাড়**"-এর ফাঁদে পা দেবেনে না। সতর্ক বিবেচনার সঙ্গে এগোবেন। ভালো করে ভেবে দেখুন কেন ২০০ টাকার জিনিস মাত্র ২০ টাকায় দেবার প্রলোভন! ভাবুন, আপনি না চাইলেও কেন আপনাকে "**বিশেষ ছাড়**"-এর প্রস্তাব দিয়ে ই-মেল পাঠানো হল?

●লটারির ধোঁকা যারা দেয় তাদের ফাঁদে পা দেবেন না। ভাবুন, অংশগ্রহণ না করেও আপনি কীভাবে লটারি জিততে পারেন?



4. SOCIAL NETWORKING RISKS

Social networking has become most popular activity in today's Internet world, with billions of people across the world using this media to meet old friends, making new friends, to collect and share information. Social networking while being a popular media has several disadvantages associated with it. These sites can be trapped by scammers or hackers leading to loss of confidentiality and identity theft, of the users. Social Networking sites are becoming very popular especially among the youth. These sites expose the kids to various risks like online bullying, disclosure of personal information, cyber-stalking, access to inappropriate content, child abuse, etc. In addition, there are many more risks like fake profiles with false information, malicious application, spam, and fake links which lead to phishing attacks etc.

Spam: Spam is usually unwanted e-mail advertising about a product sent to list of e-mails or group of e-mail addresses. Spammers send the unwanted mails or messages to the billions of users of social networking sites which are free; and are easily accessable to gather the personal information of the unsuspecting users.

Scams: Online scammers generally send an e-mail or message with a link to the user which ask for the profile information and tells the user that it would add new followers. These links sent to the user would be similar to applications, games etc. So whenever the user post his details in the link then the details will be received by scammers and information would be misused.

Phishing: Phishing attack is creation of fake site just similar to original site. These days even social networking phishing has come in different flavours just like phishing attacks on banks and popular trading websites. Social networking phishing has come up with fake mails and messages like offering some specialized themes, updating the profile, updating the security application/features etc.

৪. সোসাল নেটওয়ার্কিং-এর ঝুঁকি (Social Networking Risks)

বর্তমান বিশ্বে সোসাল নেটওয়ার্কিং ব্যবস্থা খুব জনপ্রিয় ও কার্যকরী হয়ে উঠছে। গোটা দুনিয়ায় কোটি কোটি মানুষ যেমন এতে অংশ নিয়ে পুরনো বন্ধুদের সঙ্গে যোগাযোগ করছেন, নতুন নতুন বন্ধুত্বের সম্পর্ক তৈরি করছেন এবং তথ্য আদান-প্রদান করছেন; তেমনি পাশাপাশি এর ক্ষতিকারক দিকও রয়েছে। স্ক্যামার বা হ্যাকাররা এই সাইটগুলিকে ট্র্যাপ করে ব্যবহারকারীর পরিচয় ও গোপনীয়তা নষ্ট করে ফেলতে পারে। সোসাল নেটওয়ার্কিং ব্যবস্থা বিশেষভাবে যুবসম্প্রদায়ের কাছে জনপ্রিয় হয়ে উঠছে যদিও এগুলিতে তারা নানাভাবে হয়রানির শিকার হচ্ছেন। যেমন ব্যক্তিগত তথ্য বা ঘটনা সকলের কাছে উন্মুক্ত হয়ে পড়ছে, অবাঞ্ছিত ঘটনা সকলে জেনে ফেলছে, বিয়ের প্রলোভন বা শিশু-প্রতারণার ঘটনাও বাড়ছে। এছাড়া ভুয়ো ছবি বা নাম ব্যবহার করে প্রোফাইল তৈরি করে অন্যকে ঠকানোর প্রবণতাও ব্যাপকহারে বাড়ছে।

স্প্যাম (Spam)

স্প্যাম হল কোনো পণ্য বিজ্ঞাপিত করার জন্য পাঠানো গুচ্ছমেল (Spam mail) যা একই সঙ্গে অনেককে পাঠানো হয়। এই পদ্ধতিতে স্প্যামার বা স্প্যাম-প্রচারকরা সোসাল নেটওয়ার্কিং সিস্টেম কাজে লাগিয়ে লক্ষ লক্ষ মানুষকে বিনামূল্যে নানা প্রলুব্ধকর ই-মেল বা মেসেজ পাঠিয়ে তাদের ব্যক্তিগত তথ্য সংগ্রহ করতে পারে।

স্ক্যাম (Scam)

ই-মাধ্যমে স্ক্যামাররা বা স্ক্যাম -প্রচারকরা একাধিক লিংকসহ ই-মেল ও মেসেজ পাঠিয়ে আপনার ব্যক্তিগত তথ্য জেনে নিয়ে অপব্যবহার করতে পারে। এই লিংকগুলি তারা নানারকম অ্যাপ্লিকেশন বা গেম ইত্যাদির মাধ্যমে পাঠায়।

ফিসিং (Phishing)

আসল সাইটের মত দেখতে নকল সাইট তৈরি করে প্রতারণা করার ঘটনাকে বলে ফিসিং । আজকের দিনে সোসাল নেটওয়ার্কিং সাইটের মাধ্যমে ফিসিং অ্যাটাক ঘটছে নানাভাবে। এজন্য তারা নকল ব্যাঙ্ক ও বাণিজ্যিক সাইটগুলি ব্যবহার করছে। সোসাল নেটওয়ার্কিং সাইটগুলির মাধ্যমে ভুয়ো ই-মেল ও মেসেজ পাঠিয়ে বিশেষ অফার, প্রোফাইল আপডেটিং, সিকিউরিটি অ্যাপ্লিকেশন আপডেটিং ইত্যাদির প্রস্তাব দিয়ে প্রতারণা করা হচ্ছে।

Clickjacking: Generally, clickjacking is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous Web pages. A clickjacking takes the form of embedded code or script that can run without the user's knowledge.

Malicious applications: Malicious application might come through different applications while using or installing software. Similarly, the clicking on the social networking application starts the application installation process or link to view the video, etc. In order to fulfil its intended operation the application requests for some elevated privileges from the user like access to basic information , update, post, etc. Sometimes e-mails are received with fake e-mail address like services@facebook.com by an attachment named, "Facebook_Password_4cf91.zip and includes the file Facebook_Password_4cf91exe" that, the e-mail claims, contains the user's new facebook password. When a user downloads the file, it could cause a mess on their computer and which can be infected with malicious software.

Tips to avoid risks by social networking

- Limit the information you put in the social networking sites.
- Don't put personal information like your family details, addresses, personal photographs, video, etc. In case if you put your personal photographs try to change settings and make visible only for friends
- Most of the sites and services provide options for privacy settings to prevent attackers to view your information. You can make use of these options to choose/deny whom you want to allow to see your information.
- Be careful if you want to meet social networking friends in person, sometimes it may not be their true identity which is posted on the social networking sites.
- Always think before you meet such strangers. If you decide to meet them do it in a public place during the day. Kids should never be allowed to meet such strangers alone.
- Don't ever click suspicious link while logged into social networking accounts.
- Always clean browser's cookies and cache.
- Install a good and latest version of Anti-virus to keep your system free from malicious applications like virus, worms and Trojans.
- Don't ever run any java script while logged into your social networking accounts.
- Don't ever share your password with anyone; and keep changing your password regularly. Always use proper password (min 8 digits with a mix of alpha numeric & special characters)
- Don't ever login to any site other than the legitimate sites and always check the URL for misspelled links before you proceed further.
- Use Virtual Keyboard, wherever possible to enter your password for better security as these cannot be captured by key-loggers.

ক্লিকজ্যাকিং (Clickjacking)

ক্লিকজ্যাকিং হল প্রতারণার এক কূটকৌশল যার মাধ্যমে তথ্য চুরি করে ভুয়ো ওয়েব পেজের মাধ্যমে ইন্টারনেট ব্যবহারকারীর **কম্পিউটার**ও নিয়ন্ত্রণ করা যায়। ব্যবহারকারীর অজ্ঞাতে গোপন কোডের সাহায্যে তার অসুরক্ষিত জায়গায় ঢুকে পড়ে ক্লিকজ্যাকিং-এর মাধমে হয়রান করা সম্ভব।

ক্ষতিকারক অ্যাপ্লিকেশন (Malicious Applications)

কোনো সফটওয়্যার চালু/ব্যবহার করার সময় বিভিন্ন ক্ষতিকর অ্যাপ্লিকেশন আপনার ব্যবস্থার মধ্যে চলে আসতে পারে। সোসাল নেটওয়ার্কিং সাইটে ক্লিক করলেও অনেক সময় বিভিন্ন ভিডিও ইত্যাদির সঙ্গে সংযুক্ত হয়ে যায় এবং সেই সঙ্গে নানা অপশন আসে যেগুলিতে ক্লিক করলে প্রাথমিকভাবে আপনার তথ্য স্ক্যামার বা হ্যাকারদের হস্তগত হতে পারে। কখনো কখনো সংযুক্তিসহ services@facebook.com জাতীয় ই-মেল পাঠিয়ে ব্যবহারকারীকে নতুন পাসওয়ার্ড পাঠানো হয়েছে বলে জানানো হয়। ব্যবহারকারী অসচেতনভাবে এটি ডাউনলোড করলে তার **কম্পিউটার** বা মোবাইল ক্ষতিকারক সফটওয়্যার দ্বারা আক্রান্ত হতে পারে।

সোসাল নেটওয়ার্কিং ব্যবস্থায় বিপদ এড়াবেন কীভাবে?

- সোসাল নেটওয়ার্কিং সাইটগুলিতে সীমিত তথ্য ব্যবহার করুন।
- ব্যক্তিগত ও পরিবারের বিস্তারিত তথ্য দেবেন না; দিলেও তা এমনভাবে দেবেন যাতে আপনার বন্ধুরাই কেবলমাত্র তা দেখতে পান।
- বেশিরভাগ সোসাল নেটওয়ার্কিং সাইটেই গোপনীয়তা রক্ষার জন্য যে প্রয়োজনীয় ব্যবস্থা থাকে তা ব্যবহার করে কেবলমাত্র সীমিত ব্যক্তিকেই সেগুলি দেখার অনুমতি দিন।
- সোসাল নেটওয়ার্কিং সাইটগুলিতে আপনি আপনার যে বন্ধুর সঙ্গে যোগাযোগ করতে চাইছেন তিনি সত্যিই সেই ব্যক্তি নাকি প্রোফাইলটি জাল কিনা নিশ্চিত হোন।
- এই জাতীয় সাইটে পরিচয় হওয়া ব্যক্তির সঙ্গে দেখা করবার আগে বারবার ভাবুন। দরকার মনে করলে দিনের বেলায় প্রকাশ্যস্থানে দেখা করুন। শিশুদের একা একা কোনো অচেনা-অজানা ব্যক্তির সঙ্গে দেখা করার অনুমতি দেবেন না।
- সোসাল নেটওয়ার্কিং সাইটে কোনো সন্দেহজনক লিংকে ক্লিক করবেন না।
- ভাইরাস আক্রমণ থেকে দূরে থাকার জন্য আপনার সিস্টেমে সবসময় শক্তিশালী এবং সাম্প্রতিকতম অ্যান্টি-ভাইরাস ব্যবহার করুন।
- সোসাল নেটওয়ার্কিং সাইটে থাকাকালীন জাভা স্ক্রিপ্ট ব্যবহার করবেন না।
- আপনার পাসওয়ার্ড কাউকে জানাবেন না; নিয়মিত পাসওয়ার্ড বদল করুন।
- কেবলমাত্র বৈধ সাইটেই প্রবেশ করুন। অচেনা নতুন সাইটে যাওয়ার আগে আপনার URL ঠিকঠাক চেক করুন।
- সঠিক নিরাপত্তার জন্য ভার্চুয়াল কি-বোর্ড ব্যবহার করুন এবং পাসওয়ার্ড ব্যবহারের সময় সতর্ক থাকুন।

5. ATM THREATS

The Automated Teller Machine (ATM) was first commercially introduced in the 1960s. By 2005, there were over 1.5 million ATMs installed worldwide. The ATM has enhanced the convenience of customers by enabling them to access their cash wherever required from the nearest ATM. Financial institutions have implemented many strategies to upgrade the security at their ATMs and to reduce scope for fraud. These include choosing a safe location for installing the ATM, installation of surveillance video cameras, remote monitoring, anti-card skimming solutions, and increasing consumer awareness.

RISKS

- The fraudster inserts a folded piece of plastic film into the ATM card slot so that it will hold the card and will not allow it to be expelled by the machine.
- Another method involves use of fake cards using data collected from tiny cameras and devices called "skimmers" that capture and record bank account information.
- Another interesting method of ATM frauds involves the use of "duplicate ATMs" by the fraudsters that uses software which records the passwords typed on those machines.

TIPS

- Enable your mobile phone number and e-mail with your banking transactions for timely SMS and e-mail alerts.
- Your Financial Institution or Bank will never send you an e-mail asking you to enter your Banking details online.
- Check regularly your credit card or bank account details and keep track of your transactions.
- Update your details such as change of address for receipt of cheque books, statements, debit / credit cards at the right address.
- For protecting phishing attacks, your browser should be enabled with phishing filters and never click links in your e-mail for updating and transactions.
- Keep a strong and easy to remember password and change it regularly.
- Vishing is a form of phishing, where instead of people receiving an e-mail trying to lure them into giving personal information, the criminal uses a phone call, either live or automated to attack the bank or credit union customer and get critical information.
- Try to restrict yourself from giving personal information when you receive a call from a Bank or Credit Card Provider.
- Look for a "no tampering" sign. Crooks often place these to stop anyone curious about a new piece of equipment.
- Steer clear of a jammed ATM machine that forces customers to use another ATM that has a skimmer attached. Often, the criminal will disable other ATMs in the area to draw users to the one that has the skimming device on it

- Customers should check their bank accounts regularly to make sure there are no unusual or unauthorized transactions. If you find any unauthorized ATM transactions on your bank account, immediately notify local law enforcement agency as well as your financial institution and/ or the establishment where the ATM is located.
- Always protect your PIN: Don't give the number to anyone, and cover the keypad while you are entering yours.

৫. এ টি এম-এর বিপদ-আপদ (ATM Threats)

১৯৬০ সালে বাণিজ্যিক ভাবে প্রথম এ টি এম ব্যবস্থা চালু হয়। ২০০৫ সাল পর্যন্ত সারা বিশ্বে প্রায় দেড় মিলিয়ন এ টি এম স্থাপিত হয়। প্রযুক্তির গুরুত্বপূর্ণ উন্নতির ফলে আর্থিক প্রতিষ্ঠানগুলি গ্রাহকদের সবসময় এ টি এম পরিষেবা দিয়ে চলেছে। কাছাকাছি এ টি এম থেকে গ্রাহকরা দিনের যেকোনো সময় তাদের অর্থ সংগ্রহ করতে পারছে। দুর্নীতি বন্ধ করার জন্য আর্থিক প্রতিষ্ঠানগুলি সবসময় তাদের নিরাপত্তার কৌশল বদলাচ্ছে। এজন্য তারা এ টি এম-র স্থান নির্বাচন, গোপন ক্যামেরার সাহায্যে তদারকি এবং গ্রাহকদের সচেতনতা বৃদ্ধির জন্য নানা আধুনিক পদ্ধতি উদ্ভাবন করছে।

ঝুঁকি (Risk)

●প্রতারকরা এ টি এম মেশিনে প্লাস্টিক কার্ড ঢুকিয়ে নানা ভাবে প্রতারণা করতে পারে।

●অন্য একটি পদ্ধতি হল— মেশিনে জাল কার্ড ঢুকিয়ে ব্যাঙ্ক রেকর্ড থেকে তথ্য সংগ্রহ করে প্রতারণা করা।

●নকল এ টি এম কার্ড ব্যবহার করে সফটওয়্যারের সাহায্যে মেশিনে টাইপ করা আপনার পাসওয়ার্ডটি প্রতারকরা জেনে ফেলতে পারে।

কী করণীয়

●প্রতিটি লেনদেনের তথ্য আপনি যেন ই-মেল এবং এস এম এস-র মাধ্যমে জানতে পারেন সেই পরিষেবা গ্রহণ করুন।

●মনে রাখবেন, ব্যাঙ্ক জাতীয় প্রতিষ্ঠানগুলি কখনোই অনলাইনে আপনার বিস্তারিত তথ্য জানতে চেয়ে ই-মেল পাঠায় না।

●নিয়মিত আপনার ক্রেডিট কার্ড ও ব্যাঙ্ক ব্যালেন্সে কোনো অসঙ্গতি আছে কিনা যাচাই করে দেখুন।

●সবসময় আপনার যোগাযোগের ঠিকানা আপডেটেড রাখুন যেখানে আপনার চেকবই ক্রেডিট কার্ড ইত্যাদি পাঠানো হয়।

●ফিসিং অ্যাটাক রুখতে ফিসিং ফিল্টার ব্যবহার করুন। ই-মেলে আসা লেনদেন সংক্রান্ত কোনো লিংকে ক্লিক করবেন না।

●শক্তিশালী অথচ সহজে মনে রাখা যায় এমন পাসওয়ার্ড ব্যবহার করুন এবং তা নিয়মিত বদলে নিন।

●প্রতারকরা যেন সরাসরি ফোন করে বা স্বয়ংক্রিয় কথাবার্তার (IVR) মাধ্যমে আপনার কাছ থেকে গুরুত্বপূর্ণ তথ্য জেনে নিতে না পারে সে বিষয়ে সর্বদা সজাগ থাকুন।

●ব্যাঙ্ক বা ক্রেডিট কার্ড দাতা সংস্থাকে তথ্য দেওয়ার ব্যাপারে সংযত থাকুন।

●নতুন কোনো সাজ-সরঞ্জামের বিষয়ে কোনোরকম দুর্বলতা দেখাবেন না।

●ভিড় আছে এমন এ টি এম ব্যবহারের সময় সজাগ থাকুন। এসব জায়গায় প্রতারকদের উপস্থিতি সহজ হয়। ডিভাইস (device) লাগানো আছে এমন এ টি এম ব্যবহার করতে বাধ্য করার জন্য তারা এলাকার অন্য এ টি এম গুলিকে অকেজো করে দিতে পারে।

●এ টি এম জালিয়াতির জন্য আইনি সুরক্ষায় সীমাবদ্ধতা রয়েছে। এজন্য ব্যাঙ্কগুলি সবসময় বাড়তি সুরক্ষার ব্যবস্থা করে। আপনার সুরক্ষার জন্য আপনার ব্যাঙ্কের সঙ্গে ঘনিষ্ঠ যোগাযোগ রেখে চলুন।

●এ টি এম-র আশেপাশে সন্দেহজনক কিছু দেখলে বা অবৈধ লেনদেন হলে তাড়াতাড়ি বিষয়টি উপযুক্ত কর্তৃপক্ষকে জানান।

●সবসময় আপনার পিন সুরক্ষিত রাখুন। পিন কাউকে জানাবেন না এবং পিন ব্যবহারের সময় কি-বোর্ড আড়াল করুন।

6. ONLINE BANKING

Online Banking can also be referred as Internet Banking. It is the practice of making bank transactions or paying bills through the internet. We can do all financial transactions by sitting at home or office. Online banking can be used for making deposits, withdrawals or we can even use it for paying bills online. The benefit of it is the convenience for customers to do banking transactions. The customers need not wait for bank statements, which arrive by e-mail to check their account balance. They can check their balance each and every day by just logging into their account. They can catch the discrepancies in the account and can act on it immediately.

RISKS

Link Manipulation: Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers.

Filler Evasion: Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.

Phishing Attacks: An e-mail message from a large online retailer or Internet Bank website announces that your account has been compromised and need to be updated and gives the link to update the same. So you follow a link in the message, if you click on the link it leads to the website that is as similar as original website, it is spoofed login page. If you give the account details that will be redirected to the attacker and it might be misused.

Malware attacks: Attackers try to send the malware through attachments, try to trap you by sending false e-mails with attachments saying to update your account information.

৬. অনলাইন ব্যাঙ্কিং (Online Banking)

অনলাইন ব্যাঙ্কিংকে ইন্টারনেট ব্যাঙ্কিংও বলে। এর মাধ্যমে আমরা বাড়িতে বা অফিসে বসে টাকা জমা-তোলা, বিল পেমেন্টসহ সবরকমের আর্থিক লেনদেনের কাজ করতে পারি। এর ফলে ব্যাঙ্কের কাজকর্মে অনেক সুবিধা হয়েছে। ব্যাঙ্কে কত টাকা জমা রয়েছে তা জানার জন্য এখন ব্যাঙ্ক স্টেটমেন্টের জন্য অপেক্ষা করতে হয় না। গ্রাহক কেবল তার অ্যাকাউন্টে প্রবেশ করেই তা জানতে পারেন। অতিদ্রুত তারা তাদের অ্যাকাউন্টে কোনো অসঙ্গতির বিষয়ে প্রয়োজনীয় ব্যবস্থা নিতে পারেন।

ঝুঁকি (Risk)

লিংক ম্যানিপুলেশন (Link Manipulation) ঃ প্রযুক্তির এই কৌশল ব্যবহার করে প্রতারণার ফাঁদ পাতা হয়। প্রতারকরা আপনার ই-মেলের সঙ্গে নানা লিংক জুড়ে দেয় যার ফলে আপনি অসচেতনভাবে সেখানে ক্লিক করলেই আক্রমণকারীদের ডাটাবেসে ঢুকে পড়েন এবং প্রতারিত হতে পারেন।

ফিল্টার ইভাশন (Filter Evasion) ঃ আপনি যাতে আপনার অনলাইন ব্যাঙ্কিং সিস্টেম সঠিকভাবে শোধন (ফিল্টার) করতে না পারেন সেজন্য প্রতারকেরা লেখার বদলে ছবি ব্যবহার করে নানা ট্র্যাপ পাতে।

ফিসিং অ্যাটাক (Phishing attacks) ঃ ফিসিং অ্যাটাকের মাধ্যমে অনেকসময় আসলের মত দেখতে জাল ওয়েব পেজে আপনার ব্যাঙ্ক সংক্রান্ত বিষয় আপডেট করার জন্য লিংক জুড়ে দেওয়া হয়; সেখানে আপনি ক্লিক করলেই আক্রমণকারীদের কবলে পড়ে যাবেন।

ম্যালওয়্যার অ্যাটাক (Malware attacks) ঃ আক্রমণকারীরা অনেকসময় অ্যাটাচমেন্টের সঙ্গে ম্যালওয়্যার জাতীয় ভাইরাস পাঠিয়ে আপনার অ্যাকাউন্ট ট্র্যাপ করতে পারে।

Clampi Virus Targets Users at Banks and Credit Card Sites: Keeping up with the latest Web security threats is a daunting task, because viruses and Trojans emerge, evolve, and spread at an alarming rate. While some infections like Nine Ball, Conficker, and Gumblar have hit the scene and immediately become the scourge of the cyber security world, others take their time — quietly infiltrating more and more computers before revealing the true depth of the danger they pose. One such slow grower is Clampi, a Trojan that made its debut as early as 2007 (depending on who you ask) but is only now raising hairs outside professional security circles. Clampi primarily spreads via malicious sites designed to dispense malware, but it's also been spotted on legitimate sites that have been hacked to host malicious links and ads. Using these methods, Ciampi has infected as many as half a million computers, Joe Stewart, of Secure Works, told a crowd at the Black Hat Security Conference in July, USA Today reports. Once installed on a PC, the Trojan quietly waits for you to visit a credit card or banking Web site. When it detects you're on one of the roughly 4,600 financial Web sites it's trained to watch, it records your username and password, and feeds that information back to the criminals. Clampi can even watch for network login information, allowing it to spread quickly through networked PCs (e.g., those in an office). In fact, it seems that businesses have been the primary target of Clampi so far. According to the Times Online, in July, an auto parts shop in Georgia was robbed of $75,000 when criminals stole online banking information using Clampi. The Trojan was also used to infiltrate computers for a public school district in Oklahoma and submit $150,000 in fake payroll payments.

TIPS

●Never click web links in your e-mail and no bank will ask you to update the accounts through online.
●Never provide personal information including your passwords, credit card information, account numbers to unknown persons.
●Never keep username, account name and passwords at one place. Always try to remember passwords.
●Always use phishing filters at your Internet browser.
●Do not click any images in the web sites if you are unsure.
●Confirm whether e-mail is received from bank or not.
●Be cautious while providing bank details via online, before proceed further confirm with bank about the e-mail you received. Think that if something is important or urgent why don't bank calling me instead of sending e-mail?
●Delete all cookies and history file before you perform online transactions.
●Always use virtual keyboard while accessing online banking.
●Delete all the history and cookies once you are done with online transactions.
●Avoid accessing online banking in cybercafes.

'ক্ল্যাম্পি' নামক ভাইরাসের সাহায্যে ব্যাঙ্ক ও ক্রেডিটকার্ড কোম্পানির ওয়েবসাইটে আক্রমণ (Clampi Virus Targets Users at Bank and Credit Card Sites) ঃ সবসময় সাইবার আক্রমণ ঠেকানো খুব কঠিন; কারণ ভাইরাস, ট্রোজান ইত্যাদির আক্রমণ করে ইন্টারনেটের মাধ্যমে দ্রুত ছড়িয়ে পড়ে। 'নাইন বল', 'কনফিকার', 'গাম্বলার' নামের কিছু ই-সংক্রমণ ই-বিশ্বকে ভুগিয়েছে। এর পাশাপাশি এমন কিছু ই-সংক্রামকও আছে যেগুলি চুপিসাড়ে আরো বেশিসংখ্যক **কম্পিউটার**রের গভীর বিপদ ডেকে আনতে পারে। একরম একটি শ্লথ ট্রোজানের নাম 'ক্ল্যাম্পি' যা ২০০৭ সাল নাগাদ ছড়িয়ে পড়ে বর্তমানে এক বিরাট সমস্যা হিসেবে দেখা দিয়েছে। শুরুরদিকে এটি ক্ষতিকারক সফটওয়্যার ছড়ানোর ওয়েবসাইট থেকে ছড়াতে শুরু করলেও পরে সংক্রামিত বিভিন্ন সাইট থেকেও ছড়াতে থাকে। এই ভাবে 'ক্ল্যাম্পি' প্রায় পাঁচ লক্ষ **কম্পিউটার**রে ছড়িয়ে পড়ে। ব্ল্যাকহ্যাট সম্মেলনে 'সিকিওর ওয়ার্কস'-এর মি. জো স্টুয়ার্টের মত অনুসারে 'ক্ল্যাম্পি' একবার **কম্পিউটা**রে প্রবেশ করলে সেই **কম্পিউটা**রে কোনো ব্যাঙ্ক বা ক্রেডিটকার্ড কোম্পানির ওয়েবসাইট খুললে 'ক্ল্যাম্পি' তার উপরে নজর রাখে। একসঙ্গে প্রায় ৪৬০০ এই জাতীয় ওয়েবসাইটে সে এই নজরদারি চালাতে পারে এবং আপনার আইডি ও পাসওয়ার্ড প্রতারকদের পাঠিয়ে দিতে পারে। 'ক্ল্যাম্পি' নেটওয়ার্কে দ্রুত ছড়িয়ে পড়ে আপনার কোনো নেটওয়ার্কে প্রবেশের তথ্যও পাচার করতে পারে। টাইমস অনলাইন পত্রিকা জানাচ্ছে যে 'ক্ল্যাম্পি' ব্যবহার করে জর্জিয়ার এক মোটরগাড়ি-যন্ত্রাংশের দোকান থেকে ৭৫০০০ ডলার চুরি করা হয়েছিল। ওখলাহোমার একটি সরকারি স্কুলে এই ট্রোজানটি ব্যবহার করে ১৫০০০০ ডলার ভুয়ো বেতন দেওয়া হয়েছিল।

সাবধান থাকার জন্য প্রয়োজনীয় পরামর্শ

- আপনার মেলে আসা কোনো লিংকে কখনো ক্লিক করবেন না। এটা সর্বদা মনে রাখবেন, কোনো ব্যাঙ্ক অনলাইনে আপনার অ্যাকাউন্টের আপডেট জানতে চায় না।
- কোনো অচেনা ব্যক্তিকে আপনার ব্যাঙ্কসংক্রান্ত কোনো তথ্য জানাবেন না।
- আপনার অ্যাকাউন্ট নম্বর বা পাসওয়ার্ড কোথাও লিখে রাখবেন না; তা কেবলমাত্র মনে রাখবেন।
- আপনার ইন্টারনেট ব্রাউসার সবসময় ফিসিং ফিল্টারের মাধ্যমে ফিল্টার করবেন।
- নিশ্চিত না হয়ে ওয়েবসাইটের কোনো ছবিতে ক্লিক করবেন না।
- পরবর্তী ধাপে যাবার আগে ই-মেলটি সত্যিই আপনার ব্যাঙ্ক থেকে এসেছে কিনা নিশ্চিত হোন।
- অনলাইনে ব্যাঙ্ক-তথ্য দেওয়ার সময় সতর্ক থাকুন। ভাবুন, জরুরি বিষয়ে ব্যাঙ্ক ডেকে না পাঠিয়ে মেল করল কেন?
- অনলাইন লেনদেনের আগে ও পরে সমস্ত তথ্য মুছে ফেলুন।
- সবসময় ভার্চুয়াল কি-বোর্ড ব্যবহার করুন।
- সাইবার কাফেতে অনলাইন ব্যাঙ্কিং-র কাজ না করার চেষ্টা করুন।

7. Online Shopping

Online shopping has become very popular to purchase all things without leaving your home, and it is a convenient way to buy things like electronic appliances, furniture, cosmetics, and many more. We can avoid the traffic and the crowd. We can buy at any time instead of waiting for the store to open. Apart from all these advantages risks are also there. It is very much important to take some safety measures before you go for online shopping.

Tips for safe online shopping

● Before you go for online shopping make sure that your PC is secured with all core protections like antivirus, anti spyware, firewall including system updated with all patches and web browser security.

● Before buying things, one should research about the web site from which he/she wants to buy. Attackers try to trap with websites that appear to be legitimate, but they are not. So make a note of the telephone number and physical address of the vendor and confirm that the website is a trusted site. Search for different web sites and compare the prices. Check the reviews of consumers and media of that particular web site or merchants.

● If you are ready to buy something online, check whether the site is secure like https or padlock on the browser address bar or at the status bar and then proceed with financial transactions.

● After finishing the transaction take a print or screenshot of the transaction records and details of purchase data like price, confirmation receipt, terms and conditions of the sale.

● Immediately check the credit card statements as soon as you finish online transaction. Verify about the charges you paid were same, and if you find any changes immediately report to concerned authorities.

●After finishing your online shopping, clear all the web browser cookies and turn off your PC since spammers and phishers will be looking for the system connected to the Internet and will try to send spam e-mails and will try to install the malicious software that may collect your personal information.

● Beware of the e-mails like "please confirm of your payment, purchase and account details for the product". Remember legitimate business people never send such e-mails. If you receive such e-mail immediately call the merchant and inform the same.

● A new kind of fraud attempt is being observed in the case of mobile wallets. User should be careful and should not disclose his/her PIN.

৭. অনলাইন কেনাকাটা (Online Shopping)

বাড়ির বাইরে না বেরিয়ে সবরকম জিনিস কিনতে অনলাইন কেনাকাটা এখন বেশ জনপ্রিয়। ইলেকট্রনিক যন্ত্রপাতি, আসবাবপত্র, প্রসাধনদ্রব্য এবং এরকম অনেক কিছু কিনে ফেলার সহজ পদ্ধতি হল এই অনলাইন ব্যবস্থা। রাস্তার যানজট বা ভিড় এভাবে আমরা এড়াতে পারি। দোকান খোলার অপেক্ষা না করে এভাবে যখন তখন আমরা জিনিসপত্র কিনতে পারি। এসব সুবিধে ছাড়াও অনলাইন কেনাকাটায় কিছু ঝুঁকিও আছে। অনলাইনে কেনাকাটার সময় কিছু সতর্কতামূলক ব্যবস্থা নেওয়া উচিত।

নিরাপদ অনলাইন কেনাকাটা (Tips for safe online shopping)

●অনলাইন কেনাকাটার আগে দেখে নেওয়া দরকার যে ব্যবহারের **কম্পিউটার**টি সুরক্ষিত কিনা। অর্থাৎ **কম্পিউটার**টিতে ভাইরাস প্রতিরোধী, স্পাইওয়্যার প্রতিরোধী সফটওয়্যার আছে কিনা। এছাড়া দেখতে হবে যথাযথ ওয়েব ব্রাউজার নিরাপত্তার ব্যবস্থা আছে কিনা এবং প্যাচ-এর সাহায্যে সিস্টেম সফটওয়্যারকে সুরক্ষিত করা আছে কিনা।

●কোনো ওয়েবসাইট থেকে অনলাইনে কেনাকাটার আগে সাইটটিকে যাচাই করে নিতে হবে। অবৈধ ওয়েবসাইটের সাহায্যে ব্যবহারকারীকে ফাঁদে ফেলা হয়। সুতরাং বিক্রেতার ঠিকানা ও ফোন নম্বর জেনে ওয়েবসাইটটির বিশ্বাসযোগ্যতা যাচাই করে নেওয়া উচিত। বিভিন্ন ওয়েবসাইট ঘেঁটে জিনিসের দামের তুলনা করা উচিত। ব্যবহারকারীদের মতামত ও খবরের কাগজের সমীক্ষাগুলিও এক্ষেত্রে দেখে নেওয়া যেতে পারে।

●অনলাইনে কেনাকাটার জন্য তৈরি হয়ে দেখে নিতে হয় নিরাপত্তার প্রমাণ হিসেবে https ওয়েব ঠিকানার লাইনে তালাচিহ্ন আছে কিনা।

●অর্থ লেনদেনের পরেই সেই সংক্রান্ত নথি ছাপার আকারে নিজের কাছে রাখা উচিত। এছাড়া দাম, প্রাপ্তিস্বীকার ও কেনাকাটার শর্তাবলিও হার্ডকপিতে রাখা উচিত।

●লেনদেন শেষ হওয়ার সঙ্গে সঙ্গেই ক্রেডিট কার্ডের লেনদেন সংক্রান্ত তথ্যাবলি দেখে নেওয়া দরকার এবং কিছু ভুল থাকলে তা দ্রুত সংশ্লিষ্ট কর্তৃপক্ষের নজরে আনা উচিত।

●অনলাইনে কেনাকাটার শেষে ওয়েব ব্রাউজার সৃষ্ট কুকিস মুছে ফেলা দরকার এবং ব্যবহৃত **কম্পিউটার**টি সর্বতোভাবে ও সঠিকভাবে বন্ধ করে দেওয়া দরকার। কাজের পরেও চালু **কম্পিউটার** ইন্টারনেটে যুক্ত থাকলে নানা বিপজ্জনক ব্যাপার ঘটতে পারে; এমনকি ব্যক্তিগত তথ্যও চুরি হতে পারে।

●"দয়া করে আপনার দাম মেটানো, কেনা শেষ হওয়া এবং অ্যাকাউন্ট সংক্রান্ত তথ্য আমাদের জানান"—এই জাতীয় ই-মেল থেকে সাবধান থাকুন। এই ধরনের ই-মেল বৈধ বিক্রেতারা পাঠায় না। এরকম ই-মেল পেলে সঙ্গে সঙ্গে বিক্রেতাকে ফোন করে জানানো উচিত।

●এক নতুন ধরনের প্রতারণা মোবাইল ওয়ালেট ব্যবহারে দেখা যাচ্ছে। এজন্য ব্যবহারকারীকে নিজের পিন নম্বরের গোপনীয়তা রক্ষার ব্যাপারে সদা সতর্ক থাকতে হবে।

8. MOBILE SECURITY

Providing mobile PC or mobiles to access internet for official purpose and for remote access to all business applications may put a personal or organization's vital information at risk. For professionals or individual users, using mobile or mobile PC, there are plenty of benefits such as work from anywhere, etc...The mobile devices have their own characteristics but also with security concerns such as sensitive information access with mobiles.

There are various threats, which can affect the mobile users in several ways. For example, sending multimedia messages and text messages to the toll free numbers, unknowingly clicking for a message received through the mobile phone. Now-a-days many malicious programs have come which will try to get access over mobile phones and laptops and steal the personal information inside it.

Exposure of critical information: Small amounts of WLAN signals can travel significant distance, and it's possible to peep into these signals using a wireless sniffer. A wireless intruder could expose critical information if sufficient security isn't implemented.

Lost or Stolen devices: Even if sufficient security is implemented in wireless Virtual Private Networks (VPNs), if a device is lost or stolen. the entire corporate intranet could be threatened if those devices aren't protected by a password and other user-level security measures.

Mobile Viruses: Mobile Viruses can be major threat, particularly with devices that have significant computational capabilities. Mobile devices, in general are susceptible to Viruses in several ways. Viruses can take advantage of security holes in applications or in applications or in the underlying Operating System and cause damage. Applications downloaded to a mobile device can be as Virus-prone as desktop applications. In some mobile OS, malformed SMS messages can crash the device.

Bluejacking: Bluejacking is sending nameless, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops. Bluejacking depends on the capability of Bluetooth phones to detect and contact another Bluetooth enabled device . The Bluejacker uses a feature originally proposed for exchanging contact details or electronic business cards. He or she adds a new entry in the phone's address book, types in a message, and chooses to send it via Bluetooth. The phone searches for other Bluetooth phones and, if it finds one, sends the message. Despite its name, Bluejacking is essentially harmless. The Bluejacker does not steal personal information or take control of your phone.Bluejacking can be a problem if it is used to send obscene or threatening messages or images, or to send advertising. If you want to avoid such messages, you can turn off Bluetooth, or set it to "undiscoverable".

Bluesnarfing: Bluesnarfing is the theft of data from a Bluetooth phone. Like Bluejacking, Bluesnarfing depends on the ability of Bluetooth-enabled devices to detect and contact others nearby.In theory, a Bluetooth user running the right software on a laptop can discover a nearby phone, connect to it without your confirmation, and download your phonebook, pictures of contacts and calendar. Your mobile phone's serial number can also be downloaded and used to clone the phone.You should turn off Bluetooth or set it to "undiscoverable". The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.

E-mail Viruses: E-mail Viruses affect PDAs in much the same way regular e-mail Viruses affect PCs. These Viruses are costly to enterprises and interrupt normal business too. PalmOS / LibertyCrackis an example of a PDA e-mail virus. It's a known Trojan horse that can delete all applications on a Palm PDA.

৮. মোবাইল নিরাপত্তা (Mobile Security)

ব্যক্তিগত বা সাংগঠনিকস্তরে সবরকম বাণিজ্যিক বা অফিসের কাজ মোবাইল বা ল্যাপটপের মাধ্যমে করা হচ্ছে যা খুবই ঝুঁকিপূর্ণ। অবশ্য পেশাগত বা ব্যক্তিগতজীবনে মোবাইল বা ল্যাপটপ ব্যবহারের সুবিধাও অনেক; যেকোনো জায়গায় বসেই কাজ করা যায়। মোবাইলের নিজস্ব গঠনগত বৈশিষ্ট্য থাকলেও তথ্য আদান-প্রদানে নিরাপত্তার বিষয়টিও গুরুত্বপূর্ণ।এখানেও নানাভাবে প্রতারিত ও আক্রান্ত হবার সম্ভাবনা আছে। যেমন টোল ফ্রি নম্বর থেকে বা মাল্টিমিডিয়ার মাধ্যমে মেসেজ পাঠানো হচ্ছে। না জেনে-বুঝেই মোবাইলে আসা সেসব বিষয়ে ক্লিক করলে আপনি বিপদে পড়তে পারেন। এখন মোবাইলে নানা ক্ষতিকর প্রোগ্রাম পাঠিয়ে তা গ্রহণ করানোর চেষ্টা করে ব্যক্তিগত তথ্য চুরি করা হচ্ছে।

গোপন তথ্য প্রকাশ (Exposure of critical information)

প্রয়োজনীয় নিরাপত্তা না থাকলে কিছু সংকেত ব্যবহার করে আপনার গোপন তথ্য প্রকাশ করে দেওয়া যেতে পারে। আপনার ডিভাইস হারিয়ে গেলে বা চুরি হলে তা যদি যথাযথ ভাবে পাসওয়ার্ড বা ব্যবহারজনিত অন্যান্য বিষয়ে সুরক্ষিত না থাকে তাহলে আপনার ক্ষতি হতে পারে।

মোবাইল ভাইরাস (Mobile Viruses)

কম্পিউটারের মতো সুবিধাযুক্ত মোবাইলগুলির ক্ষেত্রে ভাইরাসই হল প্রধান শত্রু। মোবাইল সাধারণত ভাইরাস বিষয়ে খুব সংবেদনশীল। ঢিলেঢালা নিরাপত্তার সুযোগে মোবাইলে ভাইরাস ঢুকে পড়ে তা অকেজো করে দিতে পারে। কোনো কিছু ডাউনলোড করার সময় ভাইরাস আপনার মোবাইলের অপারেটিং সিস্টেম নষ্ট করে দিতে পারে।

ব্লু-জ্যাকিং (Bluejacking)

ব্লু-টুথের সুবিধাযুক্ত মোবাইল বা ল্যাপটপ থেকে নামহীন অবাঞ্ছিত ম্যাসেজ পাঠানোকে ব্লু-জ্যাকিং বলে। ব্লু-জ্যাকিং নির্ভর করে একটি ব্লু-টুথের সঙ্গে অন্য ব্লু-টুথের সংযোগক্ষমতার উপর। ব্লু-জ্যাকাররা আসলে কনটাক্ট ডিটেলস বা ইলেকট্রনিক বিসনেস কার্ড ব্লু-টুথের মাধ্যমে বিনিময় করে। সাধারণভাবে এটা ক্ষতিকর না হলেও বিজ্ঞাপনের মেসেজ বা ছবি পাঠিয়ে তার মাধ্যমে কেউ আপনার ক্ষতি করতে পারে। সাবধানতা অবলম্বনের জন্য আপনার ব্লু-টুথ অদৃশ্য বা undiscoverable mode -এ রাখুন।

ব্লু-স্নার্ফিং (Bluesnarfing)

ব্লু-সার্ফিং হল ব্লু-টুথযুক্ত ফোন থেকে তথ্য চুরির পদ্ধতিবিশেষ। এটা কাছাকাছি থাকা অন্য ব্লু-টুথের সঙ্গে সংযোগক্ষমতার উপর নির্ভর করে। তত্ত্বগতভাবে একজন ব্লু-টুথ ব্যবহারকারী ল্যাপটপে সফটওয়্যার ব্যবহার করে কাছাকাছি থাকা ফোন থেকে সেই ব্যক্তির অজান্তেই মোবাইলের সিরিয়াল নম্বরসহ যাবতীয় তথ্য চুরি করে নিতে পারে। নিরাপদ থাকার জন্য আপনার ব্লু-টুথ অদৃশ্য বা undiscoverable mode-এ রাখুন।

ই-মেল ভাইরাস (E-mail Viruses)

ই-মেল ভাইরাস মোবাইল আক্রমণ করতে পারে। সাধারণ ই-মেল ভাইরাসের মতোই এই ভাইরাসের দ্বারা আপনার **কম্পিউটার** আক্রান্ত হতে পারে। এই জাতীয় ভাইরাস নিয়ন্ত্রণ করা ব্যয়বহুল এতে সাধারণ কাজকর্মে ব্যাঘাত ঘটে। লিবার্টি ক্র্যাক (Liberty Crack) হল এই ধরনের ভাইরাসের উদাহরণ। এটি Trojan horse নামেও পরিচিত যা আপনার অন্যান্য অ্যাপ্লিকেশন মুছে ফেলতে পারে।

Malicious softwares like Worms, Spywares and Trojans: Worms may disturb the phone network by spreading from one mobile to other mobile through Bluetooth transfer, Infrared transfer or through MMS attachments. Spyware that has entered into the mobile phone through Bluetooth may transfer the personal information to the outside network. The Trojan which got installed along with the game application in the mobile may send SMS messages to expansible members and may increase the phone bill.

Guidelines for securing mobile devices

●Be careful while downloading applications through Bluetooth or as MMS attachments. They may contain some harmful software, which will affect the mobile phone.
●Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops. If an unknown user tries to access the mobile phone or laptop through blue tooth, move away from the coverage area of blue tooth so that it automatically gets disconnected.
●Avoid downloading the content into mobile phone or laptop from an untrusted source.
●Delete the MMS message received from an unknown user without opening it.
●Read the mobile phone's operating instructions carefully mainly regarding the security settings, pin code settings, Bluetooth settings, infrared settings and procedure to download an application. This will help in making your mobile phone secure from malicious programs.
●Activate the pin code request for mobile phone access. Choose a pin, which is unpredictable and which is easy to remember for you.
●Use the call barring and restriction services provided by operators, to prevent the applications that are not used by you or by your family members.
●Don't make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers. It is advisable not to store important information like credit card and bank cards passwords, etc in a mobile phone.
●Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile. The operator can block a phone using the IMEI code.
●Regularly, backup important data in the mobile phone or laptop by following the instructions in the manual.
●Define your own trusted devices that can be connected to mobile phone or laptop through Bluetooth.
●Use free cleansing tools, which are available in the Internet to make your mobile work normally, whenever it is affected by malicious soft wares.

Worms ইত্যাদি ক্ষতিকারক সফটওয়্যার ব্লু-টুথের মাধ্যমে এক মোবাইল থেকে অন্য মোবাইলে ছড়িয়ে পড়ে (MMS attachment) সংযুক্তির মাধ্যমে। **Spywares** মোবাইল ফোনে ঢুকে আপনার ব্যক্তিগত তথ্য বাইরের নেটওয়ার্কে পাঠিয়ে দিতে পারে। **Trojans** গেমের মাধ্যমে আপনার মোবাইলে ঢুকে ব্যয়বহুল মেসেজ পাঠিয়ে আপনার ফোনের বিল বাড়িয়ে দিতে পারে।

আপনার মোবাইল সুরক্ষিত রাখার জন্য প্রয়োজনীয় পরামর্শ

●ব্লু- টুথের মাধ্যমে কোনো অ্যাপ্লিকেশন ডাউনলোড করার সময় সতর্ক থাকুন; এগুলির মাধ্যমে আপনার মোবাইলে ক্ষতিকারক সফটওয়্যার চলে আসতে পারে।

●দরকার না হলে মোবাইল বা ল্যাপটপে ব্লু- টুথ অদৃশ্য বা invisible mode-এ রাখুন। কোনো অচেনা ব্যক্তি ব্লু-টুথের মাধ্যমে আপনার মোবাইল বা ল্যাপটপ ব্যবহার করার চেষ্টা করলে পরিষেবাসীমার বাইরে সরে যান, যাতে করে সেটি আপনাআপনিই বিচ্ছিন্ন হয়ে যায়।

●কোনো অজানা উৎস থেকে কোনোকিছু ডাউনলোড করা থেকে বিরত থাকুন।

●অচেনা ব্যক্তির কাছ থেকে আসা MMS না খুলেই মুছে ফেলুন।

●মোবাইল ফোন ব্যবহারের নিয়মগুলি (Manual) ভালো করে পড়ুন— বিশেষত, সিকিউরিটি সেটিং, পিন সেটিং, ব্লু-টুথ সেটিং এবং কোনো অ্যাপ্লিকেশন ডাউনলোড করার পদ্ধতিগুলি। এগুলি সঠিকভাবে মেনে চললে আপনার মোবাইল ক্ষতিকারক প্রোগ্রাম থেকে দূরে থাকবে।

●মোবাইলে সবসময় পিনকোড দিয়ে রাখুন এবং তা যেন সহজে মনে রাখা যায়।

●কল (Call) নিয়ন্ত্রণের সুবিধাগুলি সংস্থার কাছ থেকে গ্রহণ করুন। আপনার বা আপনার পরিবারের যে অ্যাপ্লিকেশনগুলি দরকার হয় না সেগুলি মোবাইল থেকে (Uninstall) করুন বা সড়িয়ে ফেলুন।

●ডেবিট কার্ড বা ক্রেডিট কার্ডের গুরুত্বপূর্ণ তথ্য মোবাইলে সেভ করে রাখবেন না। আপনার মোবাইল চুরি গেলে তা থেকে আপনি প্রতারিত হতে পারেন।

●মোবাইল ফোনের IMEI Code সুরক্ষিত স্থানে লিখে রাখুন। আপনার চুরি যাওয়া মোবাইলের ব্যবহার এই কোডের সাহায্যে আটকানো সম্ভব।

●আপনার মোবাইল বা ল্যাপটপে নির্ভুলভাবে ব্লু-টুথের সংযোগ করুন।

●মোবাইল সচল ও স্বাভাবিক রাখতে ইন্টারনেট থেকে ক্লিনিং টুল ব্যবহার করুন; নতুবা আপনার মোবাইল ক্ষতিকারক সফটওয়্যার দ্বারা আক্রান্ত হতে পারে।