অফিসের ক্ষেত্রে সাইবার সচেতনতা

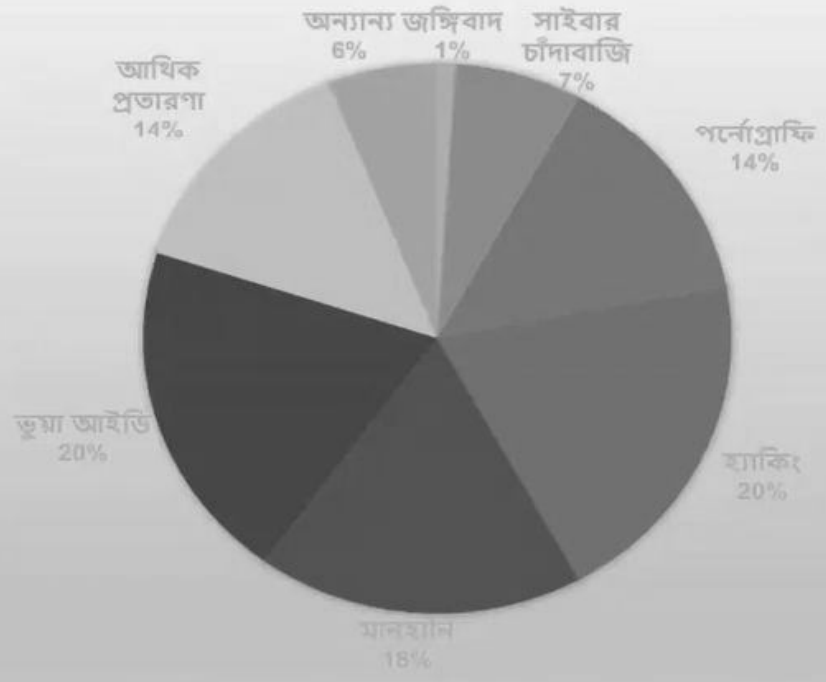
ডিজিটাল অপরাধ / Cyber Crime

যেসব যন্ত্র নেটওয়ার্ক দ্বারা একসাথে যুক্ত থাকে যেমন কম্পিউটার অথবা মোবাইল ফোন, এসব যন্ত্র ব্যবহার করে যখন কোন অপরাধ সংঘঠিত হয় তাকে ডিজিটাল অপরাধ বা সাইবার ক্রাইম বলে। সাইবার ক্রাইম, সাইবার অপরাধ বা কম্পিউটার অপরাধ, এমন এক ধরণের অপরাধ, যেখানে একটি কম্পিউটার (computer), নেটওয়ার্ক (internet) বা ইন্টারনেট সংযুক্ত ডিভাইস (device) অপরাধের সাধনের মাধ্যম হিসেবে ব্যবহার করা হয়।

সাইবার অপরাধ

বাড়ছে সাইবার অপরাধ

- সাইবার অপরাধের শিকার ৭০ ভাগই নারী।
- আক্রান্তদের বেশির ভাগের বয়সই ১৮-২৫ বছরের মধ্যে। যার ১৩% এর বয়স ১৮ এর নিচে।
- ২০১৬ সাল থেকে এ পর্যন্ত ৬৬৬ টি মামলা পর্যালোচনা করে এ তথ্য পাওয়া গেছে।



Source: Cyber Security & Crime Division, DMP

রিপোর্ট

বাড়ছে ডিজিটাল অপরাধ, বেশি শিকার নারীরা

প্রথম আলো

২৯ সেপ্টেম্বর, ২০১৯

বাংলাদেশের ইন্টারনেট ব্যবহারকারী নারীদের
৬৮ শতাংশই নানা ধরনের সাইবার
অপরাধের শিকার হচ্ছেন।

সাইবার ক্রাইম এর প্রকারভেদ

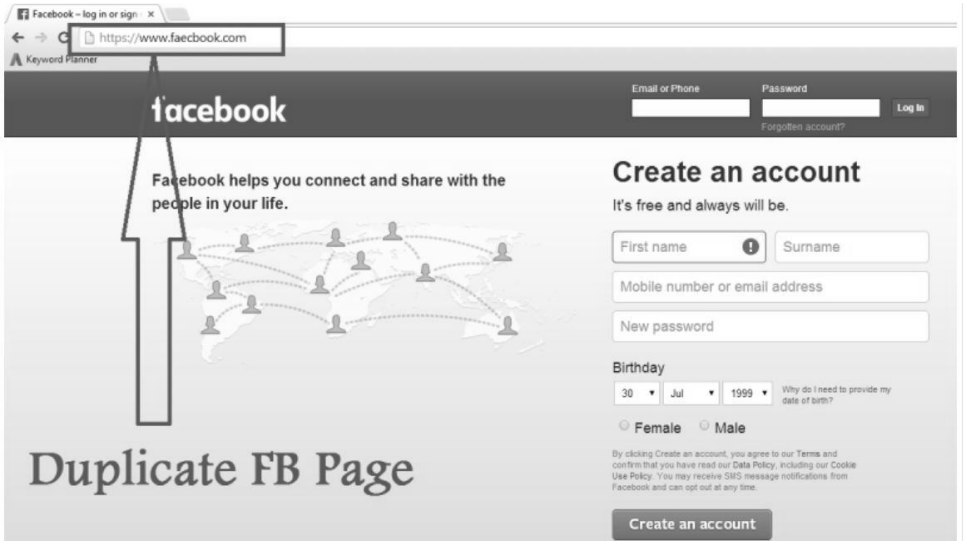
সাইবার ক্রাইমের প্রকারভেদ

ফিশিং

ফিশিং হচ্ছে এমন একটা পদ্ধতি যা ব্যবহার করে ইউজারের ব্যক্তিগত অথবা স্পর্শকাতর তথ্য পাওয়া যায়। এগুলো হতে পারে ব্যাংক অথবা ক্রেডিট কার্ডের তথ্য।

ফিশিং

ধরুন আপনার কোন এক ফ্রেন্ড আপনার ফেসবুক আইডি হ্যাক করতে চায় ফিশিং পদ্ধতির মাধ্যমে। তাহলে সে প্রথমে ফেসবুক পেইজ এর মত হুবুহু/ডুপ্লিকেট একটি নকল ফেসবুক পেইজ তৈরি করবে। যেটা দেখতে একদম অবিকল ফেসবুক পেইজ এর মত কিন্তু এর ইউআরএল হবে ভিন্ন।



সাইবার বুলিং

সাইবার বুলিং

সাইবার বুলিং বা সাইবার নির্যাতন হচ্ছে ইন্টারনেট ব্যবহার করার মাধ্যমে কাউকে অপমান করা ,হুমকি দেয়া অথবা হয়রানি করা। এই ধরনের অপরাধ ইমেইল অথবা মেসেঞ্জারের মাধ্যমে সাধারণত হয়ে থাকে।

হ্যাকিং

হ্যাকিং বলতে সে সকল কার্যক্রমকে বোঝানো হয় যার দ্বারা কারো সিস্টেমে অবৈধভাবে অনুপ্রবেশ করা হয়। হ্যাকিং এর ক্ষেত্রে, সাইবার অপরাধীরা একটি ওয়েবসাইট, কম্পিউটার বা সিস্টেম বা নেটওয়ার্ক এর ফাংশন এর ওপর সম্পূর্ণ বা আংশিক ভাবে নিয়ন্ত্রণ অর্জন করে ফেলে। এভাবে, নিয়ন্ত্রণ অর্জন করার পর তারা সেই সিস্টেম, কম্পিউটার বা নেটওয়ার্কের ব্যবহার করে বিভিন্ন অবৈধ কাজ করে নিতে পারেন।

তাছাড়া, হ্যাক করা ওয়েবসাইট, সিস্টেম বা নেটওয়ার্কে থাকা বিভিন্ন জরুরি ও ব্যক্তিগত তথ্য জেনে নিতে পারে। বেশিরভাগ ক্ষেত্রে, হ্যাকাররা corporate এবং Government account ও website এ এধরনের আক্রমন বেশী করে থাকে। যেমন; বাংলাদেশ ব্যাংকের ঘটনা ।

Identity Theft

Identity Theft

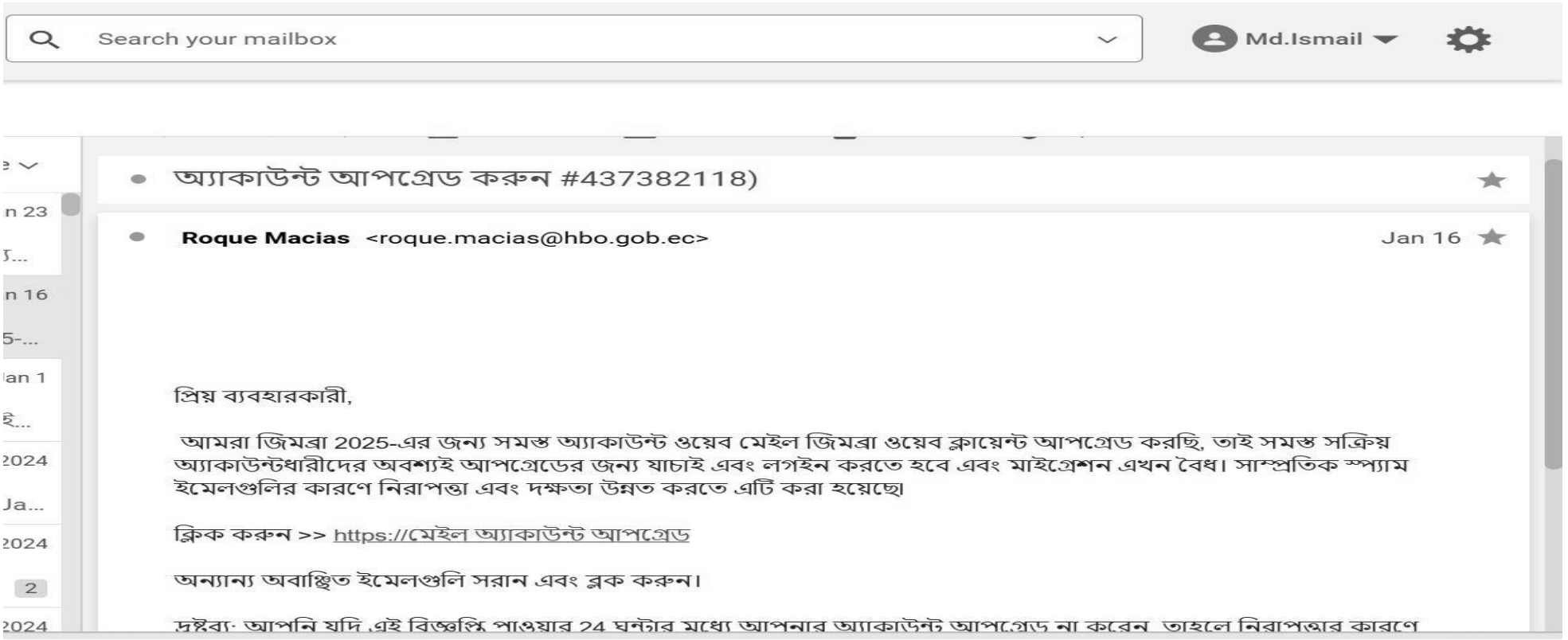
Identity theft এক ধরণের cybercrime, যেখানে ব্যক্তিগত তথ্য চুরি করা হয়। এই ব্যক্তিগত তথ্যের মধ্যে বেশিরভাগ ক্ষেত্রে account নম্বর, password, ব্যাংক একাউন্ট এর তথ্য, credit ও debit card এর তথ্য এবং এই ধরণের জরুরি এবং গোপনীয় তথ্য চুরি করা হয়ে থাকে। এই ধরণের অপরাধীরা কারো একাউন্টে থাকা টাকা চুরি করে নিতে পারে।

Scamming

স্ক্যামিং (scamming)

যেকোনো অবৈধ মাধ্যমে টাকা আয়ের উদ্দেশ্যে একজন ব্যক্তি বা সংগঠনের দ্বারা কাউকে ঠকানোকে স্ক্যামিং (scamming) বলা যেতে পারে।

Scamming


Search your mailbox
Md.Ismail
অ্যাকাউন্ট আপগ্রেড করুন #437382118)
Roque Macias <roque.macias@hbo.gob.ec>
Jan 16
প্রিয় ব্যবহারকারী,
আমরা জিমব্রা 2025-এর জন্য সমস্ত অ্যাকাউন্ট ওয়েব মেইল জিমব্রা ওয়েব ক্লায়েন্ট আপগ্রেড করছি, তাই সমস্ত সক্রিয় অ্যাকাউন্টধারীদের অবশ্যই আপগ্রেডের জন্য যাচাই এবং লগইন করতে হবে এবং মাইগ্রেশন এখন বৈধ। সাম্প্রতিক স্প্যাম ইমেলগুলির কারণে নিরাপত্তা এবং দক্ষতা উন্নত করতে এটি করা হয়েছে।
ক্লিক করুন >> https://মেইল অ্যাকাউন্ট আপগ্রেড
অন্যান্য অবাঞ্ছিত ইমেলগুলি সরান এবং ব্লক করুন।

Call Spoofing

এটি এমন এক প্রক্রিয়া যেখানে তৃতীয় ব্যক্তি আপনার ফোন হাতে না নিয়েই আপনার ফোন নাম্বার থেকে অন্য কাউকে কল করতে পারবে।

Call Spoofing কিভাবে কাজ করে? → এটি মূলত VoIP (Voice over internet protocol) দ্বারা পরিচালিত হয়ে থাকে। আমরা সাধারণত টাওয়ার ব্যবহার করে কল দিয়ে থাকি আর VoIP সিস্টেম ইন্টারনেট ব্যবহার করে কল দিয়ে থাকে। অনেকে হোয়াটসঅ্যাপ বা মেসেঞ্জার কলের প্রসেসকে VoIP সিস্টেমের অন্তর্ভুক্ত মনে করে থাকলে ভুল করবেন। VoIP সিস্টেমে একজন ইন্টারনেট ব্যবহার করে কথা বলে টাওয়ার ব্যবহার করে কথা বলা আরেকজনের সঙ্গে। VoIP কলের সুবিধা হলো এখানে কলার ইচ্ছামত যে কোন একটি নাম্বার সেট করে কল করতে পারে, কিন্তু সেটা বেআইনি। তারা SIP প্রটোকলের মাধ্যমে নিজের একটি প্রোভাইডার স্টেশন তৈরি করে, সেখান থেকে ইচ্ছেমতো যেকোনো নাম্বার সেট করে যেকোনো কাউকে কল দেওয়া যায়।যেমন: আপনার বাবার নাম্বার সেট করে কেউ কল দিল এবং আপনার ফোনে সে কলটি আসলো, আপনার বাবার নাম্বার থেকে ফোন এসেছে, তারমানে ফোনটা আপনার বাবা-ই করেছেন বলে আপনি মনে করবেন। কিন্তু আসলে তৃতীয় ব্যক্তি ফোনটি করেছে।

Computer Virus

Computer virus

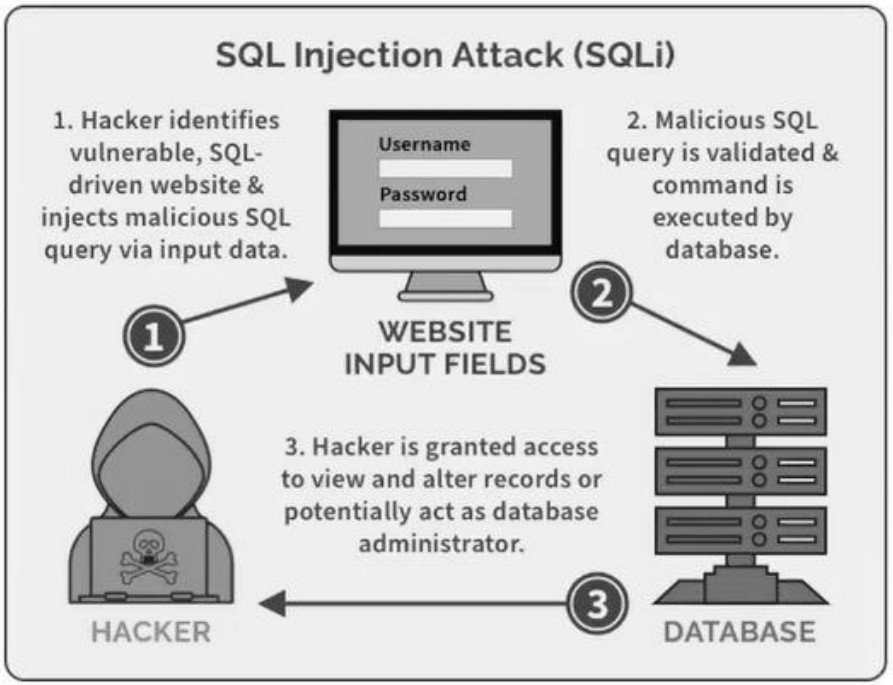
কম্পিউটার ভাইরাস এর সাহায্যে কম্পিউটার সিস্টেমে ঢুকে অবৈধ ভাবে ব্যক্তিগত এবং আর্থিক তথ্য চুরি করে, নষ্ট করে বা নিয়ন্ত্রণ নিয়ে নেয়। সাইবার অপরাধীরা কম্পিউটার সিস্টেম বা নেটওয়ার্ক এ বিভিন্ন রকমের virus যেমন malware, Trojan ইত্যাদি পাঠিয়ে কম্পিউটার সিস্টেমকে সংক্রমিত বা নষ্ট করে দিতে পারে। বেশিরভাগ ক্ষেত্রে এই ধরণের virus গুলো internet এবং removable device থেকে কারো network বা computer system এ ঢুকে যেতে পারে।

Ransomware

Ransomware

এটি এক ধরনের malware-virus attack যেখানে অপরাধীরা কারো কম্পিউটার নেটওয়ার্কে ঢুকে সেখানে থাকা জরুরি file গুলো এনক্রিপ্ট করে রাখে। এবং পরবর্তীতে অর্থের বিনিময়ে তা উন্মুক্ত করে দেয়।

SQL Injection



SQL Injection হলো হলো এমন এক কৌশল, যার মাধ্যমে ওয়েব সাইটের ডাটাবেস এ প্রবেশাধিকারের জন্য ক্ষতিকর (malicious) কোড প্রবেশ করানো। এই কৌশল প্রয়োগ করে একজন হ্যাকার আপনার ডেটাবেজকে ধ্বংস করে দিতে পারে বা নিয়ন্ত্রণ নিয়ে নিতে পারে। ওয়েবপেজ এর মাধ্যমে ডেটাবেজে ক্ষতিকর (malicious) কোড ইনপুট/জমা করাই হলো SQL Injection

ডিজিটাল অপরাধ সংঘটনের কারন

- ✓ আর্থিক লাভের (Monetary Gain) হওয়া;
- ✓ ব্যক্তি, প্রতিষ্ঠান বা রাষ্ট্রের ক্ষতিসাধন;
- ✓ গুরুত্বপূর্ণ তথ্য হাতিয়ে নেয়া;
- ✓ কম্পিউটার ও তথ্যপ্রযুক্তি ব্যবহারকারীদের অসচেতনতা, অসতর্কতা ও অদক্ষতা;
- ✓ ডিজিটাল আইন সম্পর্কে পর্যাপ্ত জ্ঞানের অভাব;
- ✓ এছাড়াও কিছু কিছু ডিজিটাল অপরাধের ক্ষেত্রে ক্ষতিগ্রস্ত ব্যক্তির আইনি ব্যবস্থা গ্রহণে অনাগ্রহ ইত্যাদি

ডিজিটাল অপরাধ সংঘটনের অন্যতম প্রধান কারণ।

সাইবার অপরাধ থেকে সুরক্ষার পদ্ধতি

১. শক্তিশালী পাসওয়ার্ড: শক্তিশালী পাসওয়ার্ড এবং মাল্টি-ফ্যাক্টর অথেনটিকেশন ব্যবহার করা উচিত, যাতে অননুমোদিত প্রবেশের ঝুঁকি কমে।

২. অ্যান্টি-ম্যালওয়্যার এবং ফায়ারওয়াল: সাইবার অপরাধ থেকে সুরক্ষা পেতে অ্যান্টি-ম্যালওয়্যার সফটওয়্যার এবং ফায়ারওয়াল ব্যবহার করা উচিত, যা সিস্টেমে ক্ষতিকারক সফটওয়্যার অনুপ্রবেশ করতে বাধা দেয়।

৩. ইমেইল এবং লিঙ্ক যাচাই: সন্দেহজনক ইমেইল, লিঙ্ক, বা ফাইল খোলার আগে তা যাচাই করা উচিত এবং ফিশিং আক্রমণ থেকে সতর্ক থাকা উচিত।

৪. ব্যাকআপ: গুরুত্বপূর্ণ ডেটার নিয়মিত ব্যাকআপ রাখা উচিত, যাতে সাইবার আক্রমণের ফলে ডেটা হারিয়ে গেলে তা পুনরুদ্ধার করা যায়।

সাইবার সিকিউরিটি কি?

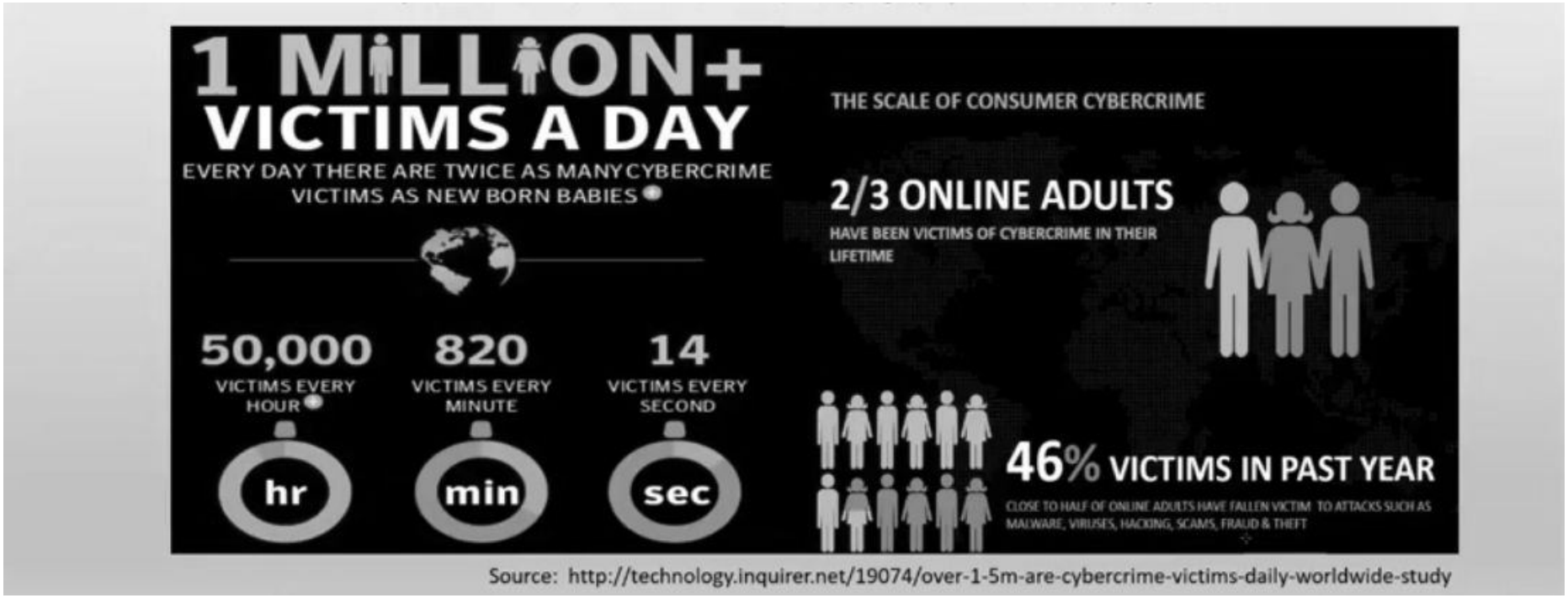
- সাইবার সিকিউরিটি হলো এমন একটি প্রক্রিয়া, যেখানে বিভিন্ন আধুনিক প্রযুক্তির মাধ্যম computer device, data, network এবং program গুলোকে cyber attack, cybercrime এবং অবৈধ ব্যবহার থেকে সুরক্ষিত করে রাখা হয়।
- এক কথায় computer, device বা network গুলোকে সাইবার অপরাধীদের থেকে নিরাপদে রাখার প্রক্রিয়া কে বলা হয় সাইবার সিকিউরিটি।

সাইবার ট্রাইবুনাল

- ✓ সাইবার ট্রাইব্যুনালে চলমান **মামলার ৬০** শতাংশ মামলাই ফেসবুকে নারীদের নিয়ে আপত্তিকর ছবি এবং অশ্লীল ভিডিও ইন্টারনেটে ছেড়ে দেওয়ার অপরাধ সংক্রান্ত।

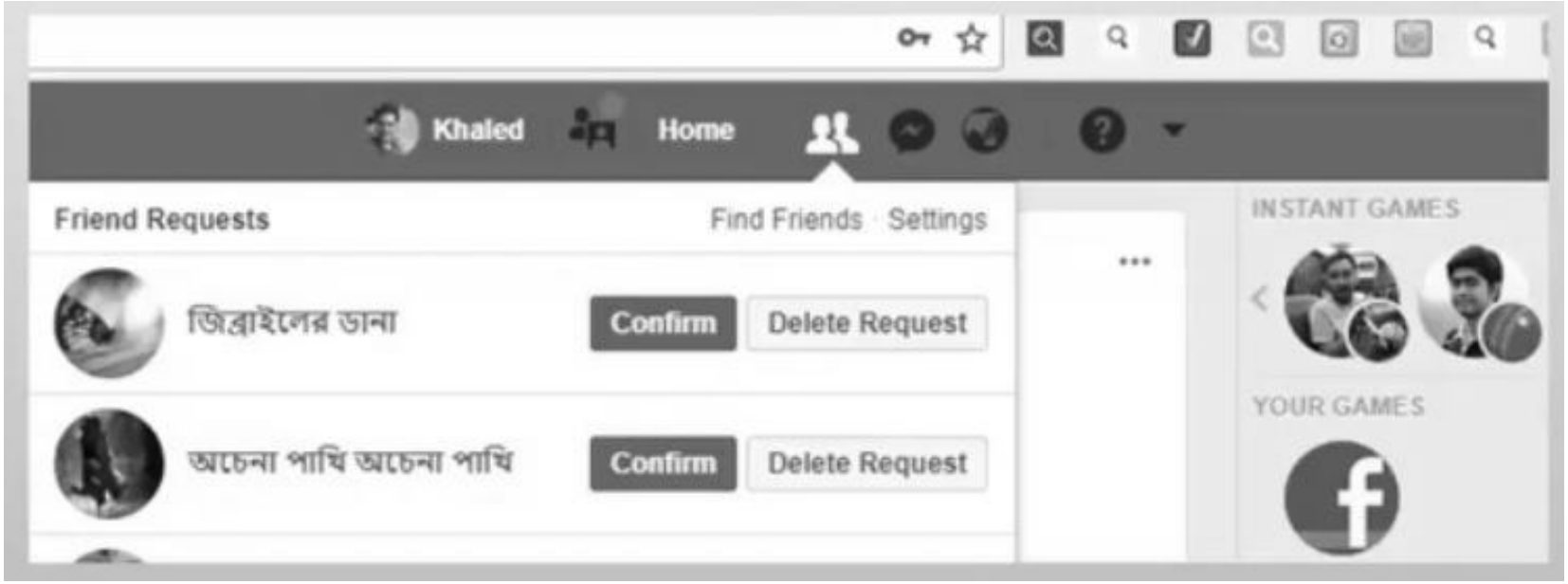
- ✓ সিসিএ কার্যালয়ে প্রেরিত **৫০ টি মামলার** মধ্যে ৪৩ টি মামলাই সামাজিক যোগাযোগ মাধ্যম সংক্রান্ত।

পরবর্তী ডিজিটাল অপরাধের শিকার কে ?



নিজেকে কিভাবে রক্ষা করব?

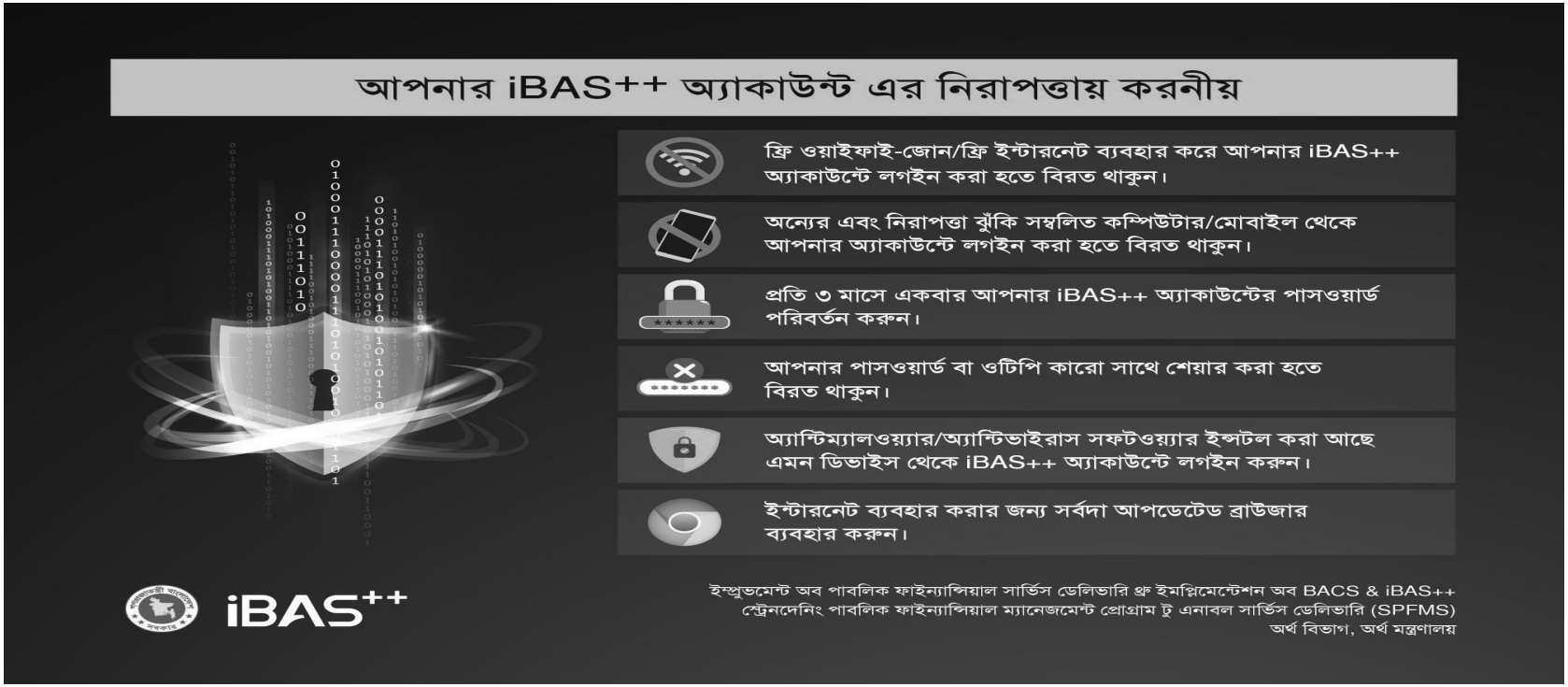
কতটুকু চেনেন?


Khaled
Home
Friend Requests
Find Friends
Settings
জিব্রাইলের ডানা
Confirm
Delete Request
অচেনা পাখি অচেনা পাখি
Confirm
Delete Request
INSTANT GAMES
YOUR GAMES

অপরিচিত লিঙ্ক


Zoom Bangla News
November 28, 2017
জ্যাককে কেন বাঁচানো হয়নি ব্যাখ্যা দিলেন নির্মাতা
জ্যাককে কেন বাঁচানো হয়নি ব্যাখ্যা দিলেন নির্মাতা - ZoomBangla News
Priyo
11 hrs
মার্কিন যুক্তরাষ্ট্রের মাই ফিটনেস প্যাল নামের একটি খাদ্য ও পুষ্টিসংক্রান্ত অ্যাপ থেকে সম্প্রতি চুরি হয়েছে কমপক্ষে ১৫ কোটি মানুষের তথ্য।
ফিটনেস অ্যাপ থেকে ১৫ কোটি মানুষের তথ্য চুরি
মার্কিন যুক্তরাষ্ট্রের মাই ফিটনেস প্যাল নামের একটি খাদ্য ও পুষ্টিসংক্রান্ত অ্যাপ থেকে চুরি হয়েছে কমপক্ষে ১৫ কো.....

নিজেকে কিভাবে রক্ষা করব



সাইবার নিরাপত্তার পূর্বশর্ত

- ব্যক্তিগত পর্যায়ে সচেতনতা তৈরি
- পারিবারিক ও প্রাতিষ্ঠানিক শিক্ষা প্রদান
- প্রযুক্তিগত সক্ষমতা
- আইনের কঠোর প্রয়োগ

থামো...

ভাবো...

সংযোগ দাও

পাসওয়ার্ড সুরক্ষা


You can share a cup of ice cream
But don't share your password
Strength matters
7zcd@1s3
Protect yourself choose a password that is hard to crack
Just like diapers,
Passwords need to be changed regularly.

কম্পিউটারের নিরাপত্তা

- কম্পিউটারে এন্টি ভাইরাস করা
- নিজের ডিভাইসের পাসওয়ার্ড শেয়ার না করা;
- নিরাপদ/লাইসেন্সড সফটওয়্যার ব্যবহার করুন;
- ক্লোনড ও পাইরেটেড সফটওয়্যার ব্যবহার না করা।

ই-মেইল এর নিরাপত্তা

•একাউন্ট রিসেট বা আপগ্রেড করার জন্য কোনো লিংকে ক্লিক না করা;

•শক্তিশালী পাসওয়ার্ড ব্যবহার করুন এবং সর্বোর্চ্চ ০৩ (তিন) মাসের মধ্যে পাসওয়ার্ড পরিবর্তন করা;

•ই-মেইল বা মেসেজের মাধ্যমে অর্থ প্রাপ্তি , লটারি বা পুরস্কার জেতার কথা বললে বিশ্বাস না করা।

ব্রাউজার নিরাপত্তা

- ✓ব্রাউজার নিয়মিত হালনাগাদ করা ;
- ✓কোনো ওয়েবসাইটে লগইন করার আগে ওয়েব এড্রেস যাচাই করা;
- ✓অনলাইন একাউন্টে লগইন করার সময় ওয়েব এড্রেস https/Secure কিনা যাচাই করা;
- ✓অনলাইন একাউন্টে প্রয়োজনে One Time Password (OTP)/ Two Factor Authentication সিস্টেম চালু করা;
- ✓ইন্টারনেট ব্যবহারের সময় নতুন অপশন এলে যাচাই করে সেগুলোতে প্রবেশ করা;
- ✓যে সকল গেমস ইন্টারনেট সংযোগ ছাড়াই খেলা যায় সেগুলো খেলার সময় ইন্টারনেট সংযোগ বন্ধ রাখা;
- ✓শুধু শিক্ষামূলক ও নির্ভরযোগ্য সাইটগুলো ব্যবহার করা;
- ✓ব্রাউজারের কিছু অপশন প্রয়োজনে নিষ্ক্রিয়/ সক্রিয় করে রাখা; যেমন: popup block, site block

সামাজিক যোগাযোগ মাধ্যমের নিরাপত্তা

- ✓ফেসবুক এবং অন্যান্য সোশ্যাল মিডিয়ার নিরাপত্তা সেটিংস নিয়মিত যাচাই করা ;
- ✓সোশ্যাল মিডিয়া একাউন্টের ই-মেইল/এসএমএস নোটিফিকেশন চালু করে নেয়া;
- ✓কোনো পোস্ট প্রকাশ করার আগে কে পোস্টটি দেখতে পারে তা যাচাই করে নেয়া;
- ✓অধিকতর নিরাপত্তার জন্য আপনার সোশ্যাল মিডিয়ার একাউন্টে মোবাইল নম্বর নিবন্ধন করা;
- ✓একাউন্টে টু ফ্যাক্টর অথেনটিকেশন সিস্টেম চালু রাখা;
- ✓অনলাইনে অপরিচিত কারো সাথে বন্ধুত্ব করার ক্ষেত্রে সতর্ক থাকা;
- ✓যত কাজেরই হোক না কেন, কারো অনুরোধে ওয়েব ক্যামেরা বা মোবাইল ফোনের ক্যামেরার সামনে কোন ধরনের শারীরিক অঙ্গ-ভঙ্গি কিংবা অঙ্গ প্রদর্শন করা থেকে বিরত থাকা;

ওয়াইফাই ব্যবহারের সতর্কতা

- ✓ প্রোফাইল পেজে গিয়ে অ্যাকটিভিটি লগ নিয়মিত যাচাই করা
- ✓ নিজের ব্যক্তিগত তথ্য, ছবি, ও ভিডিওচিত্র শেয়ার করা থেকে বিরত থাকা
- ✓ অনলাইনে কেউ উত্ত্যক্ত করলে বা সন্দেহজনক আচরণ করলে তা বাবা-মাকে জানানো।
- ✓ বাবা-মার সাথে বন্ধুত্বপূর্ণ সম্পর্ক বজায় রাখা যাতে তাদের সাথে সবকিছু শেয়ার করা যায় এবং প্রয়োজনে সহযোগিতা পাওয়া যায়।

ওয়াইফাই নেটওয়ার্ক ব্যবহারে সতর্কতা

- ✓ পাবলিক প্লেসে ফ্রি ওয়াইফাই নেটওয়ার্ক ব্যবহার করা থেকে বিরত থাকা;
- ✓ অনলাইন আর্থিক লেনদেন করার ক্ষেত্রে ফ্রি ওয়াইফাই নেটওয়ার্ক ব্যবহার করা থেকে বিরত থাকা।

মোবাইল ব্যাংকিং নিরাপত্তা

১. নিজের মোবাইল ব্যাংকিং একাউন্টের পিন নম্বর ও একাউন্ট ব্যালেন্স অপরকে না জানানো;

২. ফোনে অপরিচিত কেউ যদি আপনাকে ভুল করে টাকা পাঠানোর কথা বলে টাকা ফেরত চায় তাহলে তাকে টাকা ফেরত না পাঠানো। কোন ম্যাসেজ দ্বারা প্রভাবিত হয়ে কাউকে টাকা ফেরত না পাঠানো। সেক্ষেত্রে আগে মূল একাউন্ট ব্যালেন্স চেক করা।

৩. কখনও লটারি জেতার কথা শুনে কোন টাকা-পয়সা লেনদেন না করা

৪. ফোনে কখনও কারো কথায় বা কারো নির্দেশনায় কোনো নম্বরে ডায়াল না করা বা ব্যক্তিগত তথ্য প্রদান না করা বা টাকা না পাঠানো।

ডিজিটাল সাইন

ডিজিটাল স্বাক্ষর

বাংলাদেশে ইলেক্ট্রনিক কার্যক্রমে নিরাপত্তা ও ব্যক্তির পরিচিতি নিশ্চিতকরণের লক্ষ্যে তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ মোতাবেক ডিজিটাল স্বাক্ষর ও ডিজিটাল সনদ চালু করা হয়।

Anonymity of Internet

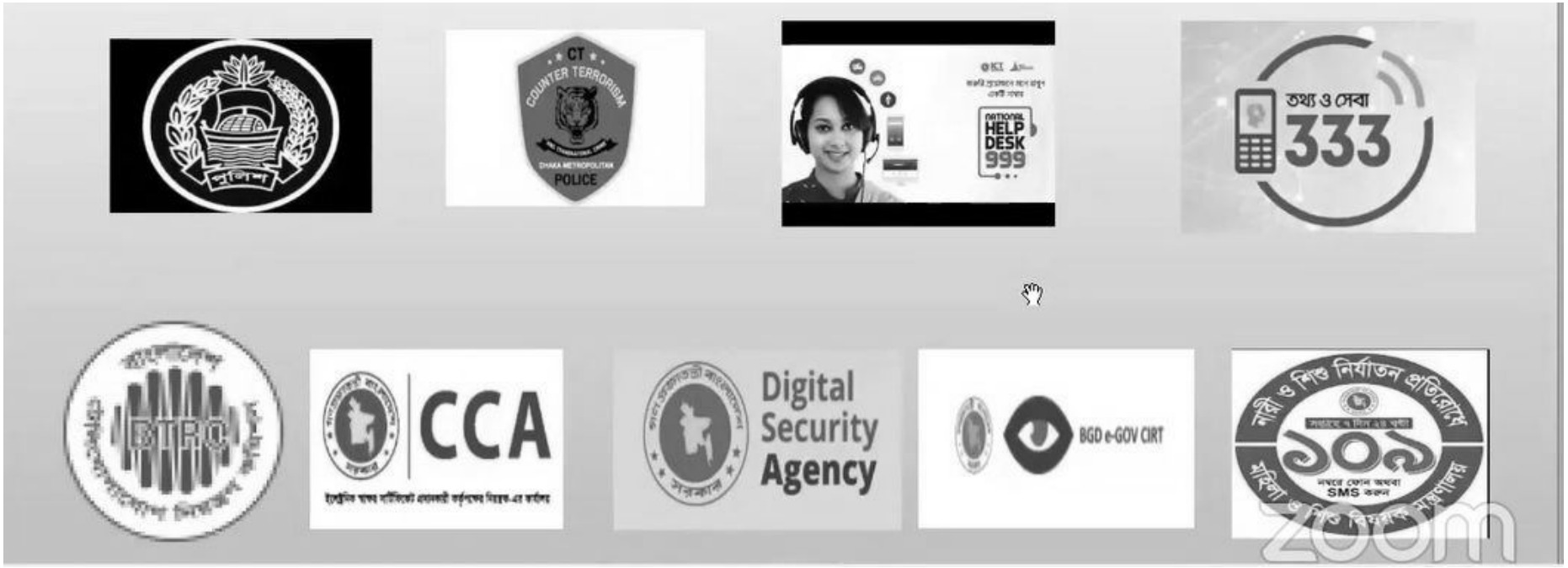
Anonymity of the Internet drives tendency towards abuse

"On the Internet, nobody knows you're a dog."

আপনার ফেসবুক আইডি হ্যাক ও রিপোর্টিং

✓ লিংক (https://www.facebook.com/hacked) খুলুন।
✓'My Account is compromised' বাটনে ক্লিক করুন।
✓পরবর্তী ধাপে আপনার নিজ প্রোফাইলের অন্তর্ভূক্ত 'Email Address' অথবা 'Phone number' লিখে 'Search' বাটনে ক্লিক করুন।
✓ফেসবুক কর্তৃপক্ষ আপনার একাউন্টের 'পাসওয়ার্ড' পরিবর্তন করার অনুরোধ করবে
✓ একটি Security code আপনার 'Email Address' অথবা 'Phone number' এ যাবে।
✓ নতুন 'পাসওয়ার্ড' এর জন্য অনুরোধ করবে
✓ এবং আপনার সাম্প্রতিক 'লগ-ইন' কর্মকান্ড পর্যালোচনা করবে।

কোথায় জানাবেন?

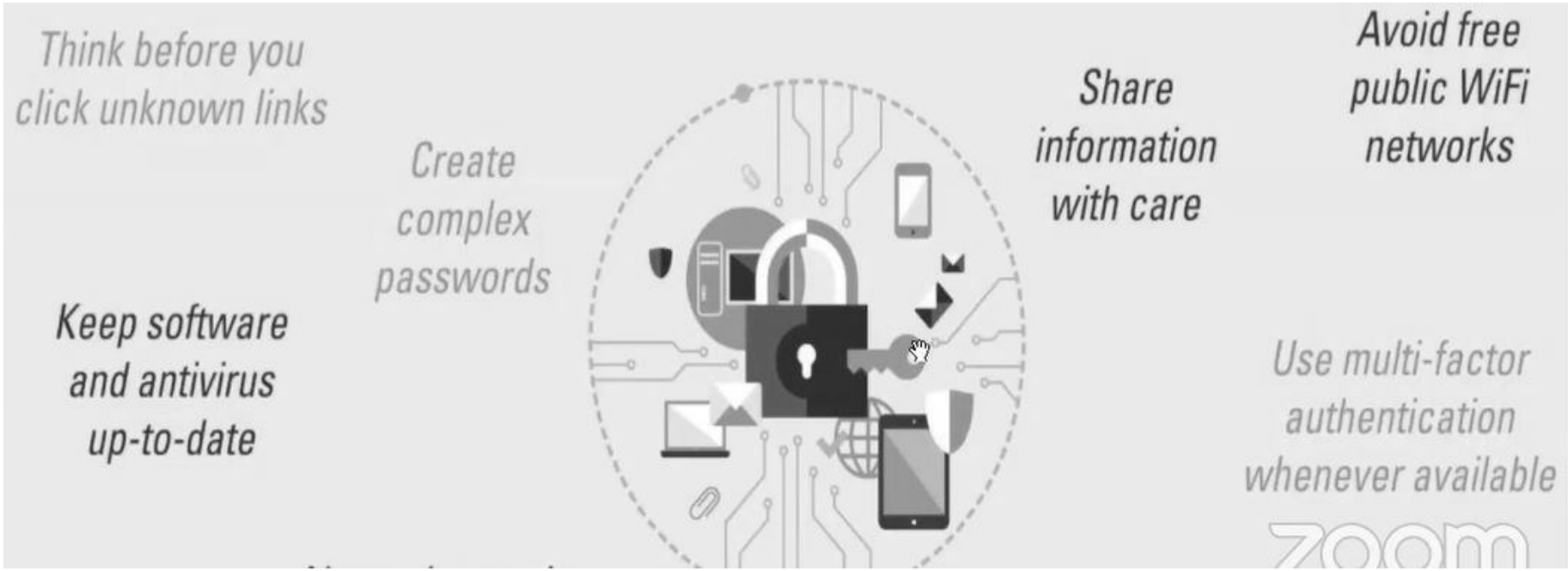

CT
COUNTER TERRORISM
DHAKA METROPOLITAN
POLICE
NATIONAL
HELP
DESK
999
তথ্য ও সেবা
333
CCA
Digital
Security
Agency
BGD e-GOV CIRT
১০৯
SMS করুন

অনলাইন মাধ্যম নির্যাতন/হয়রানির প্রমান সংরক্ষণ

- ✓হার্ডকপি রাখতে হবে।
- ✓URL সহ স্ক্রিন শট প্রিন্ট করে রাখতে হবে।
- ✓বিভিন্ন ওয়েব অ্যাড্রেস (URL), ফেসবুক আইডি, ই-মেইল আইডি ও তারিখ সংরক্ষণ করতে হবে।
- ✓যত বেশী সম্ভব প্রমাণ সংরক্ষণ করতে হবে।

Think Before Clicking

Remember Again



ডিজিটাল দুনিয়ায় সচেতন থাকুন
নিজেকে নিরাপদ রাখুন।

নিরাপদ ডিজিটাল পরিবেশ গড়ি
সুরক্ষিত থাকুক বাংলার নারী

বর্তমান অবস্থা

বর্তমান দুনিয়ায় বুলেটের জায়গা
দখল করে নিচ্ছে বাইট

ইন্টারনেট দুনিয়ায় আপনার
প্রতিটি ক্লিক হোক নিরাপদ

ধন্যবাদ