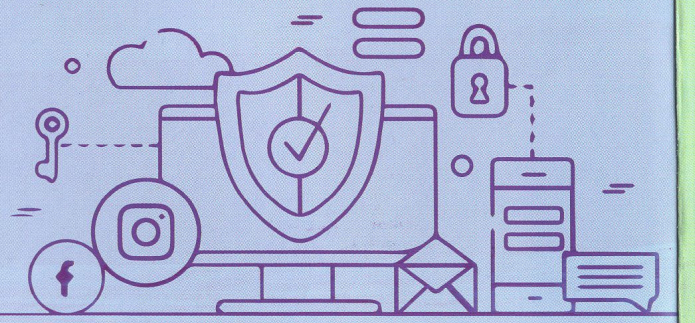
গোপনীয় বা ব্যক্তিগত কন্টেন্ট ফেসবুকে ছেড়ে দেয়া হলে করণীয়

কারো কোন গোপনীয় বা ব্যক্তিগত কন্টেন্ট ফেসবুকে ছেড়ে দেয়া হলে ফেসবুক কর্তৃপক্ষের কাছে রিপোর্ট করতে হবে। এক্ষেত্রে যা করণীয়:

- ❑ যে পোস্টের মাধ্যমে গোপনীয় বা ব্যক্তিগত কন্টেন্ট ফেসবুকে শেয়ার করা হয়েছে সে পোস্টের ডানদিকে রিপোর্ট করার অপশনে গিয়ে Find support or report post এ ক্লিক করতে হবে।
- ❑ অপশনে থাকা বিভিন্ন ইস্যু যেমন- Fake news, violence, harassment ইত্যাদির মধ্য থেকে উপযুক্ত বিষয়টি নির্বাচন করতে হবে।
- ❑ ভুক্তভোগী নিজে কিংবা তাঁর ফেসবুক বন্ধুরা Me/My friends থেকে উপযুক্ত অপশনটি নির্বাচন করে মিথ্যা বা মানহানীকর পোস্টটির বিরুদ্ধে রিপোর্ট করতে পারেন।
- ❑ সংশ্লিষ্ট পোস্টটির সম্পূর্ণ লিঙ্কসহ স্ক্রিনশট নিয়ে সংরক্ষণ করে রাখতে হবে যা পরবর্তীতে যেকোন আইনী পদক্ষেপ নিতে সহায়ক হবে।
- ❑ গোপনীয় বা ব্যক্তিগত কনন্টেন্ট ফেসবুকে ছড়িয়ে পড়ার মাধ্যমে হয়রানি কিংবা বিড়ম্বনার শিকার হলে কালক্ষেপণ না করে নিকটস্থ থানা পুশিকে অবহিত করতে হবে।

[তথ্যসূত্র: www.police.gov.bd]



সাইবার ক্রাইম এর শিকার হলে নিম্নবর্ণিত যে কোন হেল্প ডেস্কের সহযোগিতা নেয়া যাবে

১। **সাইবার ক্রাইম ইনভেস্টিগেশন ডিভিশন**
কাউন্টার টেরোরিজম এন্ড ট্রান্সন্যাশনাল ক্রাইম, ডিএমপি
৩৬, মিন্টো রোড, রমনা, ঢাকা
হেল্পডেস্ক নম্বর: ০১৭৬৯৬৯১৫২২
ইমেইল: cyberhelp@dmp.gov.bd

২। **সাইবার পুলিশ সেন্টার, সিআইডি**
ফোন: ০১৩২০০১০১৪৮
ইমেইল: https://cid.gov.bd/

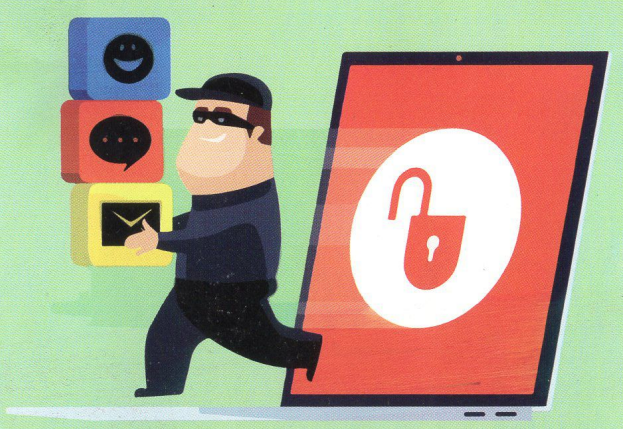
৩। **ফেসবুক পেইজ-পুলিশ সাইবার সাপোর্ট ফর উইমেন (পিসিএসডব্লিউ)**
ফোন নাম্বার: ০১৩২০০০০৮৮৮
ইমেইল: cybersupport.women@police.gov.bd

৪। **হ্যালো সিটি এ্যাপস (ডাউনলোড ফ্রম গুগল প্লে স্টোর)**

৫। **রিপোর্ট টু র‍্যাব এ্যাপস (ডাউনলোড ফ্রম গুগল প্লে স্টোর)**

৬। **৯৯৯**

৭। **এছাড়াও নিম্নোক্ত পেইজে সংযুক্ত থাকা যেতে পারে-**
http://www.police.gov.bd,
facebook.com/cyberctdmp,
facebook.com/dmpdhaka,
facebook.com/cpccidbdpolice



এসো সুরক্ষিত থাকি অনলাইনে

সচেতনতায়

বাংলাদেশ পুলিশ উইমেন নেটওয়ার্ক
(বিপিডব্লিউএন)

সাইবার ক্রাইম বা সাইবার অপরাধ কাকে বলে?

তথ্যপ্রযুক্তি ও ইন্টারনেট ব্যবহার করে অনলাইনে যে অপরাধসমূহ সংঘটিত হয় তাকে সাইবার অপরাধ বা সাইবার ক্রাইম বলে। প্রযুক্তির সহজলভ্যতা বিশ্বের অপার জ্ঞানভান্ডারকে উন্মুক্ত করে দিয়ে যেমন অভাবনীয় উন্নয়নের দ্বার উন্মোচন করেছে তেমনি ইন্টারনেটকে কেন্দ্র করে নানাবিধ অপরাধ কৌশল উদ্ভাবনের ফলে 'নেটওয়ার্কভিত্তিক অপরাধ বা সাইবার ক্রাইম' এর মাত্রা আশঙ্কাজনক হারে বৃদ্ধি পাচ্ছে।

বাংলাদেশে প্রায়শই ঘটা সাইবার অপরাধসমূহের মধ্যে রয়েছে আইডি হ্যাকিং, উগ্র ও বিদ্বেষপূর্ণ মন্তব্য/অডিও/ভিডিও প্রচার, ফেইক অ্যাকাউন্ট তৈরী, সাইবার বুলিং বা হ্যারাসমেন্ট, প্রশ্নপত্র ফাঁস, ডেবিট ও ক্রেডিট কার্ড জালিয়াতি, অনলাইন মাল্টি লেভেল মার্কেটিং ও গ্যাম্বলিং ইত্যাদি। তাই অনলাইনে সুরক্ষিত থাকতে হলে আমাদের সাধারণ কিছু নিরাপত্তামূলক ব্যবস্থা গ্রহণ করা প্রয়োজন।

অনলাইনে নিরাপদ থাকার জন্য সাধারণ সতর্কতা

- ব্যক্তিগত ফোন/ল্যাপটপ বা অন্য যে কোন পাবলিক ডিভাইসে অনলাইন মাধ্যম ব্যবহারের পর যথাযথভাবে লগআউট হতে হবে।
- লটারী/মূল্য হ্রাস বা কোন আকর্ষণীয় সুবিধা প্রদানের প্রস্তাব দিয়ে কোন লিঙ্ক প্রেরণ করা হলে সেই লিঙ্কে ক্লিক করা থেকে বিরত থাকতে হবে, ইমেইলে বা ইনবক্সে প্রেরিত কোন অপরিচিত এ্যাটাচমেন্ট ওপেন করা যাবে না।
- অপরিচিত কাউকে ফ্রেন্ডস লিস্টে এ্যাড করা যাবে না। অনলাইনে পরিচিত হওয়া কোন ব্যক্তি কোন স্থানে দেখা করতে চাইলে তা এড়িয়ে চলতে হবে।
- নিজের ব্যবহৃত পুরোনো ফোন/ল্যাপটপ অন্য কারও ব্যবহারের উদ্দেশ্যে দেয়ার সময় নিজের সকল ব্যক্তিগত তথ্য ভালোভাবে ডিলিট করতে হবে।
- সকল সোশ্যাল মিডিয়া একাউন্টের সিকিউরিটি অপশনে থাকা প্রাইভেসি সেটিংস নিয়ন্ত্রণ করতে হবে। নিজের ব্যক্তিগত তথ্যের এ্যাকসেস সবার কাছে দেয়া যাবে না।
- একই পাসওয়ার্ড একাধিক সোশ্যাল মিডিয়া একাউন্টের জন্য ব্যবহার করা থেকে বিরত থাকতে হবে।
- অপরিচত কারও সাথে অনলাইনে চ্যাট করা, ব্যক্তিগত ছবি শেয়ার করা বা কোন সম্পর্কে জড়ানো নিরাপদ নয়। ব্যক্তিগত কোন মূহুর্তের ছবি কোন ডিভাইসে সংরক্ষণ করা যাবে না।
- সাইবার বুলিং এর উদ্দেশ্যে কেউ আপত্তিকর মেসেজ পাঠালে তার উত্তর না দিয়ে বা প্রতিক্রিয়া না দেখিয়ে স্ক্রিনশট নিতে হবে এবং পুলিশের সহযোগিতা চাইতে হবে।
- 'Google Yourself'- গুগলে নিজের নাম সার্চ দিয়ে দেখতে হবে আপত্তিকরভাবে কোথাও নিজের নাম বা ছবি ব্যবহার করা হয়েছে কি না।
- কোন একাউন্ট থেকে বিব্রতকর ছবি বা মেসেজ পাঠানো হলে সে একাউন্ট ব্লক করে দিতে হবে।
- সোশ্যাল মিডিয়ায় ধর্মীয় অনুভূতিতে আঘাত দিয়ে বা অন্যের অধিকারকে ক্ষুণ্ন করে কোন মন্তব্য করা যাবে না। সঠিকভাবে যাচাই না করে কোন ধরনের গুজব বা মিথ্যা তথ্য শেয়ার করা যাবে না।
- ব্যবহার্য সকল ডিভাইসে ভালো মানের এন্টিভাইরাস সফ্টওয়ার ব্যবহার করতে হবে।

ফেসবুক একাউন্টের নিরাপত্তা বিধানে করণীয়

- সহজে অনুমানযোগ্য পাসওয়ার্ড ব্যবহার না করে শক্তিশালী পাসওয়ার্ড ব্যবহার করতে হবে। ব্যক্তিগত তথ্য যেমন: জন্ম তারিখ, নিজের নাম, শিক্ষা প্রতিষ্ঠানের নাম ইত্যাদি পাসওয়ার্ড হিসেবে ব্যবহার করা থেকে বিরত থাকতে হবে।
- Capital letter, small letter, number & symbol মিলিয়ে শক্তিশালী পাসওয়ার্ড ব্যবহার করতে হবে। পাসওয়ার্ডকে অনেকটা টুথব্রাশের মত ব্যবহার করতে হবে- আমরা যেমন একটি ভালো টুথব্রাশ বেছে নেই, কারও সাথে তা শেয়ার করিনা এবং অন্তত তিন মাস পর পর তা পরিবর্তন করি, ঠিক একইভাবে পাসওয়ার্ড কারও সাথে শেয়ার করা যাবে না এবং নির্দিষ্ট সময় পর তা পরিবর্তন করতে হবে।
- Two factor authentication অপশন চালু রাখতে হবে (ফেসবুকের সেটিংস থেকে Security & login > use two-factor authentication এ গিয়ে মোবাইল নম্বর কিংবা ইমেইল যুক্ত করতে হবে) অন্য কেউ লগইন করতে চাইলেও এই ইমেইলে বা মোবাইল নাম্বারে আসা কোড জানতে পারবে না বিধায় সুরক্ষিত থাকা যাবে।
- জন্ম তারিখ, ফোন নাম্বারসহ অন্যান্য ব্যক্তিগত তথ্য উন্মুক্ত রাখা যাবে না। এতে বিভিন্ন রকমের হয়রানি ও প্রতারণা থেকে নিজেকে মুক্ত রাখা সহজ হবে।
- ফেসবুকের ক্ষেত্রে Trusted Contact-এ ৩ থেকে ৫ জন বিশ্বস্ত ফেসবুক বন্ধুকে যুক্ত রাখতে হবে। এর ফলে আইডি হ্যাক হয়ে গেলেও তা উদ্ধার করা সহজ হবে।
- ফেসবুকের Privacy Settings- অপশনটি ব্যবহারের মাধ্যমে ব্যক্তিগত তথ্য, ছবি, পোস্টের নিরাপত্তা নিশ্চিত করতে হবে। প্রয়োজনে প্রোফাইল লক করে রাখতে হবে।
- স্ট্যাটাস বা ব্যক্তিগত ছবি প্রাইভেসি নিশ্চিত করে শেয়ার করতে হবে। ফেসবুকে নিজের জীবনাচরণ যত বেশি উন্মুক্ত হবে তত বেশি ঝুঁকি থাকবে।
- ফেসবুক একাউন্ট খোলার সময় জাতীয় পরিচয়পত্রের সাথে সামঞ্জস্যপূর্ণ নাম ও জন্ম তারিখ ব্যবহার করতে হবে। এতে আইডি হ্যাক হলে আইনী ব্যবস্থা গ্রহণ করা সহজ হবে।

ফেসবুক একাউন্ট হ্যাক হলে করণীয়

- প্রথমেই http://www.facebook.com/hacked লিঙ্কে প্রবেশ করতে হবে।
- এরপর "Someone else got into my account without my permission"- এ ক্লিক করতে হবে। হ্যাক হওয়া একাউন্টটির তথ্য চাওয়া হলে সেখানে উল্লেখ করা ২টি অপশনের (ইমেইল বা ফোন নম্বর) যে কোন একটির ইনফরমেশন দিতে হবে।
- এরপর "My account is compromised" এ ক্লিক করতে হবে। হ্যাক হওয়া একাউন্টটির তথ্য চাওয়া হলে সেখানে উল্লেখ করা ২ টি অপশনের (ইমেইল বা ফোন নম্বর) যে কোন একটির ইনফরমেশন দিতে হবে।
- প্রদত্ত তথ্য সঠিক হলে প্রকৃত একাউন্টটিই দেখাবে এবং বর্তমান অথবা পুরাতন পাসওয়ার্ড চাইবে; এখানে পুরাতন পাসওয়ার্ড টি দিয়ে "Continue" করতে হবে।
- হ্যাকার যদি ইমেইল এ্যাড্রেস পরিবর্তন করে না থাকে তাহলে আগের ইমেইলে রিকভারি অপশন পাঠানো হবে। এর মাধ্যমে হ্যাকড ফেসবুক একাউন্ট উদ্ধার করা সম্ভব।
- হ্যাকার যদি ইমেইল এ্যাড্রেস, ফোন নম্বরসহ লগইন এর জন্য প্রয়োজনীয় তথ্য পরিবর্তন করে থাকে তাহলে, Need another way to authenticate? > Submit a request to Facebook এ ক্লিক করলে ফেসবুক প্রোফাইলটি উদ্ধারের জন্য প্রয়োজনীয় তথ্য ও আইডি সরবরাহের ফর্ম পূরণের মাধ্যমে হ্যাকড ফেসবুক এ্যাকাউন্ট উদ্ধার করা সম্ভব।

[তথ্যসূত্র: www.police.gov.bd]