Australian Government

এখনই ব্যবস্থা নিন।
নিরাপদে থাকুন।

অনলাইনে কীভাবে নিরাপদ থাকতে পারেন

সহজে পড়তে পারার সংস্করণ

Easy Read

এই নির্দেশিকাটি ব্যবহারের পদ্ধতি

আমরা অস্ট্রেলিয়ার সরকার।

আমরা এই নির্দেশিকাটি লিখেছি।

আমরা কিছু শব্দ **মোটা (বোল্ড)** করে লিখেছি।

আমরা এই শব্দগুলোর অর্থ ব্যাখ্যা করবো।

এই শব্দগুলোর একটি তালিকা ৩১নং পৃষ্ঠায় দেওয়া আছে।

আপনি বিশ্বস্ত কারো কাছে নিম্নোক্ত বিষয়ে সাহায্য চাইতে পারেন:

- এই নির্দেশিকাটি পড়তে
- আরও তথ্য খুঁজে পেতে।

এটি অন্য একটি নির্দেশিকার সহজে পড়তে পারার জন্য সংক্ষিপ্ত সংস্করণ।

এতে শুধুমাত্র সবচেয়ে গুরুত্বপূর্ণ বিষয়গুলো আছে।

আপনি অন্য নির্দেশিকা টি আমাদের ওয়েবসাইটে পাবেন।

www.actnowstaysecure.gov.au

এই নির্দেশিকাতে কী আছে?

এই নির্দেশিকা সম্পর্কে 4

আপনার অ্যাকাউন্ট নিরাপদ রাখুন 6

আপনার তথ্য সুরক্ষিত রাখতে আপনার সেটিংস পরীক্ষা করুন 10

আপনার ডিভাইসসমূহ সুরক্ষিত রাখুন 16

প্রতারণা 20

সাহস করে বলুন 25

শব্দের তালিকা 28

আমাদের সাথে যোগাযোগ করুন 30

এই নির্দেশিকা সম্পর্কে

আমরা অনলাইনে কীভাবে নিরাপদে থাকতে পারবো এ বিষয়ে আমাদের সবার চিন্তা করে উচিত।

একে আমরা বলি **সাইবার** নিরাপত্তা।

সাইবার অর্থ হলো ইন্টারনেটের সাথে সম্পর্কিত।

অনলাইনে নিজেকে নিরাপদ রাখার জন্য কিছু বিষয় এই নির্দেশিকাতে ব্যাখ্যা করা হয়েছে।

যেমন, **সাইবার অপরাধ (Crime)** থেকে নিরাপত্তা।

সাইবার অপরাধ হলো যখন অপরাধীরা তাদের অপরাধের জন্য ইন্টারনেট ব্যবহার করে।

যেমন, তারা নিম্নোক্ত কাজগুলো করতে ইন্টারনেট ব্যবহার করতে পারে:

- আপনার ব্যক্তিগত তথ্য চুরি
- আপনার অনলাইন অ্যাকাউন্ট বা প্রোফাইলের দখল নিয়ে নেওয়া।

সাইবার অপরাধ যেকোনো ডিভাইসেই হতে পারে।

এর মধ্যে আছে আপনার:

- কম্পিউটার
- স্মার্টফোন
- স্মার্ট ওয়াচ।

সাইবার অপরাধ থেকে নিরাপদ থাকার জন্য আপনি কিছু কাজ করতে পারেন।

আপনি কী কী করতে পারেন তা আমরা পরের পৃষ্ঠাগুলোতে ব্যাখ্যা করেছি।

আপনার অ্যাকাউন্ট নিরাপদ রাখুন

আপনি আপনার অনলাইন অ্যাকাউন্টগুলো কীভাবে সুরক্ষিত রাখতে পারবেন তা নিয়ে আপনার চিন্তা করা উচিত।

শক্তিশালী ও ভিন্ন ভিন্ন পাসফ্রেজ ব্যবহার করুন।

পাসওয়ার্ড এর আরও শক্ত ধরনই হলো **পাসফ্রেজ (passphrase)**।

এটি অন্য কারও পক্ষে অনুমান করা খুবই কঠিন।

আপনার অ্যাকাউন্ট সুরক্ষিত রাখার অন্যতম ভালো পদ্ধতি হলো শক্ত ও ভিন্ন ভিন্ন পাসফ্রেজ ব্যবহার করা।

আপনার প্রত্যেক অনলাইন অ্যাকাউন্ট এর জন্য আলাদা আলাদা পাসফ্রেজ ব্যবহার করা উচিত।

শক্তিশালী পাসফ্রেজ এ নিম্নোক্ত জিনিসগুলি থাকে:

- ৪টি বা তার বেশি এলোমেলো শব্দ
- ১৫টি বা তার বেশি অক্ষর ও সংখ্যা।

আপনি এর মধ্যে কিছু বড় হাতের অক্ষর দিতে পারেন।

আপনি আরও কিছু চিহ্নও ব্যবহার করতে পারেন, যেমন:

- ড্যাশ
- ডলার চিহ্ন
- ইমেইল এর অ্যাট (@) চিহ্ন।

আপনার পাসফ্রেজ এ কোনো ব্যক্তিগত তথ্য রাখা উচিত নয়।

যেমন:

- আপনার জন্মদিন
- আপনার পরিবারের সদস্য বা পোষা প্রাণীদের নাম।

আপনার অ্যাকাউন্টে ঢুকতে (লগ ইন করতে) বাড়তি ধাপ যোগ করুন

মাল্টি ফ্যাক্টর অথেনটিকেশন (এমএফএ) এর মাধ্যমে আপনি আপনার অনলাইন একাউন্ট সুরক্ষিত করতে পারেন।

অ্যাকাউন্টে প্রত্যেকবার লগ ইন করার সময় ২ বা ততোধিক ভাবে লগ ইন করাকে এমএফএ বলে।

উদাহরনস্বরুপ, আপনাকে প্রথমে পাসফ্রেজ দিতে হতে পারে।

এরপর আপনার ফোনে আসা একটি কোড দিতে হতে পারে।

আপনাকে নিম্নোক্ত ধাপগুলোর মধ্যে বাছাই করতে দেওয়া হতে পারে:

- কোড এর জন্য আপনার ফোনে একটি অ্যাপ নেওয়া

- একটি ইমেইলে কোড পাওয়া

- একটি এসএমএস এ কোড পাওয়া।

অন্য কেউ আপনার অ্যাকাউন্টে ঢোকাকে এমএফএ কঠিন করে তোলে।

যদিও বা তারা আপনার পাসফ্রেজ জেনে যায়।

আপনার তথ্য সুরক্ষিত রাখতে আপনার সেটিংস পরীক্ষা করুন

আপনার সেটিংস কি অনলাইনে আপনার তথ্য সুরক্ষিত রাখছে কিনা আপনি পরীক্ষা করতে পারেন।

এর মধ্যে আছে আপনার:

- অনলাইন অ্যাকাউন্টসমূহ
- ডিভাইসসমূহ
- অ্যাপস।

আপনি এগুলো করতে পারেন:

- সেটিংস বদলানো
- কোন কোন অ্যাপ আপনার তথ্য ব্যবহার করবে যা বাছাই করা।

আপনি আপনার ডিভাইসে সেটিংস খুঁজে পেতে পারেন:

- গিয়ার চিহ্নটি খুঁজে

  অথবা

- আপনার ডিভাইসের সার্চ বারে "settings" লিখে।

মেনু (Menu) খোলার মাধ্যমে আপনি কোন অ্যাপ বা অনলাইন অ্যাকাউন্ট এর সেটিংস খুঁজে পেতে পারেন।

সাধারণত ৩টি সোজা দাগ দিয়ে মেনু দেখানো হয়।

এই সেটিংসগুলো কিছু কিছু ক্ষেত্রে এই বিষয়গুলো সম্পর্কে তথ্য প্রকাশ করতে পারে:

- আপনি কে
- আপনি কোথায় আছেন
- আপনি কোথায় থাকেন।

এই তথ্যগুলো অনলাইনে প্রকাশ করার মাধ্যমে আপনাকে সাইবার অপরাধের ঝুঁকিতে ফেলতে পারে।

সাইবার অপরাধীরা আপনার তথ্য ব্যবহার করে আপনি হওয়ার ভান করতে পারে।

যেমন, তারা নিম্নোক্ত তথ্যগুলো ব্যবহার করতে পারে:

- আপনি কোথায় থাকেন

- আপনার পরিবারের সদস্যদের নাম

- আপনার পোষা প্রাণীদের নাম।

আপনি আপনার অ্যাকাউন্ট এমনভাবে সেট করতে পারেন যেনো শুধুমাত্র আপনার পরিচিত মানুষরাই আপনার সামাজিক মাধ্যমের প্রোফাইল দেখতে পারে।

যেমন, আপনার ফেসবুক প্রোফাইল।

এই সেটিংস গুলোকে সাধারণত প্রাইভেসি সেটিংস বলা হয়।

আপনি আপনার **লোকেশন সেটিংস** ও নিয়ন্ত্রণ করতে পারবেন।

আপনার ডিভাইসটি কোথায় আছে তা দেখা যায় লোকেশন সেটিংস এর মাধ্যমে।

আপনি লোকেশন সেটিংস খোলা বা বন্ধ (on or off) করতে পারেন।

কোন কোন অ্যাপ আপনার লোকেশন সেটিংস ব্যবহার করতে পারবে তাও আপনি বাছাই করে দিতে পারেন।

আপনি নিম্নোক্ত সব কিছুর জন্য এটি করতে পারেন:

- অনলাইন অ্যাকাউন্ট
- ডিভাইস
- অ্যাপস।

কিছু অ্যাপ এই বিষয়ে আপনার অনুমতি চাইতে পারে:

- আপনার ক্যামেরা ব্যবহার করার মাধ্যমে

- আপনার ছবি দেখাতে।

শুধুমাত্র পরিচিত অ্যাপকেই আপনার ক্যামেরা ও ছবি ব্যবহার করতে দেওয়া উচিত।

আপনার ডিভাইসসমূহ সুরক্ষিত রাখুন

অনলাইনে নিরাপদ থাকার জন্য আপনি কিভাবে আপনার যন্ত্রপাতি সুরক্ষিত রাখবেন তা নিয়ে আপনার চিন্তা করা উচিত।

যেমন, আপনার ফোন বা স্মার্ট ওয়াচ।

ইন্টারনেটে সংযুক্ত সব ডিভাইসসমূহের জন্য এটি গুরুত্বপূর্ণ।

আপনার ডিভাইসসমূহ আপডেট করুন

আপনার ডিভাইসসমূহ অনলাইনে নিরাপদ রাখার জন্য সেগুলো আপডেট করতে পারেন।

যেমন, আপনার ফোন ও ল্যাপটপ।

আপনার ডিভাইস এটিকে সফটওয়ার আপডেট বলতে পারে।

আপডেট করার মাধ্যমে একটি ডিভাইস সাইবার অপরাধ থেকে নিজেকে সুরক্ষা করতে সহায়তা করে।

আপনি কোনও ডিভাইসকে নিজে নিজে আপডেট হতে সেট করে রাখতে পারেন।

আপনার ডিভাইসসমূহকে কিভাবে আপডেট করতে হয় সে সম্পর্কে আমাদের ওয়েবসাইটে আরো জানতে পারবেন।

www.actnowstaysecure.gov.au/cyber-safe-actions

পাবলিক ওয়াই-ফাই নেটওয়ার্ক

পাবলিক ওয়াই-ফাই ব্যবহার করার সময় আপনাকে সতর্ক থাকতে হবে।

সবার ব্যবহারের জন্য উন্মুক্ত করে রাখা ফ্রি ওয়ারলেস ইন্টারনেটকে বলা হয় পাবলিক ওয়াই-ফাই।

উদাহরনস্বরুপ:

- ক্যাফেতে
- এয়ারপোর্টে
- হোটেলে।

পাবলিক ওয়াই-ফাই ব্যবহার করে কোন ওয়েবসাইটে কি তথ্য দিচ্ছেন এ বিষয়ে আপনাকে সাবধান থাকতে হবে।

যেমন, আপনার:

- ব্যাংক সম্পর্কিত তথ্য
- ইমেইল অ্যাকাউন্ট
- সামাজিক যোগাযোগের প্রোফাইল।

কিছু কিছু সাইবার অপরাধী পাবলিক ওয়াই-ফাই ব্যবহার করতে পারে:

- আপনি অনলাইনে কী করছেন দেখতে
- আপনার তথ্য চুরি করতে।

কারণ:

- এটি যে কেউ ব্যবহার করতে পারে

- এতে আপনার ডিভাইসসমূহ সুরক্ষিত রাখা কঠিন।

আমাদের ওয়েবসাইটে আপনি পাবলিক ওয়াই-ফাই ব্যবহারের সময় নিরাপদ থাকা সম্পর্কে আরো জানতে পারবেন।

www.actnowstaysecure.gov.au/cyber-safe-actions

প্রতারণা

কেউ যদি নিচের কাজগুলো করার চেষ্টা করে তাকে আমরা **প্রতারণা (scam)** বলি:

- আপনাকে ঠকানো
- আপনার টাকা নেওয়া।

যারা প্রতারণা করে তাকে আমরা **প্রতারক (scammer)** বলি।

প্রতারকরা আপনাকে নিম্নোক্ত পদ্ধতিতে ঠকানোর চেষ্টা করতে পারে:

- এসএমএস বা ফোন কল
- ইমেইল
- সামাজিক যোগাযোগ মাধ্যম
- ওয়েবসাইট।

তাদেরকে বন্ধুত্বপূর্ণ মনে হতে পারে।

কিন্তু তারা আপনাকে ঠকিয়ে আপনার তথ্য নিয়ে নিতে পারে।

তারা এটি ব্যবহার করতে পারে:

- আপনার অনলাইন অ্যাকাউন্টে ঢুকতে

- আপনার ছদ্মবেশ ধারণ করতে

- আপনার টাকা চুরি করতে।

প্রতারকরা আরও করতে পারে:

- আপনাকে ঠকানোর জন্য মিথ্যা অ্যাকাউন্ট বানানো

- আপনি ক্লিক করার জন্য লিংক বা বিজ্ঞাপন দেওয়া।

প্রতারণাকে কীভাবে শনাক্ত করবেন

এটি প্রতারণা হতে পারে যদি:

- আপনাকে তাড়াতাড়ি কিছু করতে বলে

- আপনাকে অনেক টাকা দিতে চায়

- আপনার কাছে টাকা চায়

- আপনাকে কোনো লিংকে ক্লিক করতে বলে।

প্রতারকরা আপনার পরিচিত ও বিশ্বস্ত কোনো প্রতিষ্ঠান হওয়ার ভানও করতে পারে।

যেমন, আপনার ব্যাংক।

প্রতারকরা এই কাজটি করে যেনো আপনি তাদেরকে আপনার ব্যক্তিগত তথ্য প্রদান করেন।

আপনার কাউকে প্রতারক মনে হলে আপনি তাদের সাথে কথা বলা বন্ধ করা উচিত।

কেউ আপনাকে যে পরিচয় দিচ্ছে সেটি সঠিক নাকি আপনার পরীক্ষা করা উচিত।

আপনি বিশ্বাস করেন ও নিজে খুঁজে বের করেছেন এমন যোগাযোগের ঠিকানায় সেই ব্যক্তি বা প্রতিষ্ঠানের সাথে যোগাযোগের চেষ্টা করতে পারেন।

কোনো কিছু সন্দেহজনক মনে হলে নিজেকে সুরক্ষা করার জন্য তাড়াতাড়ি পদক্ষেপ নিন।

প্রতারণা রিপোর্ট করা

Scamwatch অস্ট্রেলিয়ানদের সাহায্য করে:

- প্রতারণা বুঝতে
- প্রতারণা রিপোর্ট করতে।

Scamwatch প্রতারণার শিকার হওয়া অস্ট্রেলিয়ানদেরও সহায়তা করে।

আপনি Scamwatch এর ওয়েবসাইটে কোনো প্রতারণার ব্যাপারে রিপোর্ট করতে পারেন।

www.scamwatch.gov.au/report-a-scam

সাহস করে বলুন

অন্যরা কীভাবে নিজেকে অনলাইনে নিরাপদ রাখবে এ সম্পর্কে আপনার কথা বলা উচিত।

এর মধ্যে আছে:

- সাইবার অপরাধ রিপোর্ট করা

- আপনি যা জানেন তা আপনার পরিবার ও বন্ধুবান্ধবকে জানানো।

আপনি কিভাবে সাহস করে কথা বলতে পারেন তা আমরা নিচে ব্যাখ্যা করবো।

সাইবার অপরাধ রিপোর্ট করুন

সাইবার অপরাধ রিপোর্ট করার মাধ্যমে সরকারকে নিম্নোক্ত ব্যাপরে সহায়তা করা যায়:

- সাইবার অপরাধীরা কীভাবে আক্রমণ করার চেষ্টা করে তা শেখা

- আরও বেশী মানুষকে নিরাপত্তা দেওয়া।

আপনি ReportCyber এর ওয়েবসাইটে কোনো সাইবার অপরাধ রিপোর্ট করতে পারেন।

www.cyber.gov.au/report

অনলাইনে নিরাপদ থাকা সম্পর্কে পরিবার ও বন্ধুবান্ধবকে জানানো

অনলাইনে নিরাপদ থাকা সম্পর্কে আপনার পদ্ধতিগুলো পরিবার ও বন্ধুবান্ধবকে জানানো উচিত।

আপনিও তাদের থেকে শিখতে পারেন।

অনলাইনে নিরাপদ থাকা সম্পর্কে আপনি যা যা জানেন, তা আপনার আশেপাশের সবাইকে জানানোর মাধ্যমে আপনি নিজেকে ও অন্য সবাইকে সুরক্ষিত করতে পারেন।

এটি গুরুত্বপূর্ণ যদি আপনি অন্য কারও সাথে আপনার ডিভাইসসমূহ শেয়ার করেন।

শব্দের তালিকা

এই নির্দেশিকায় **মোটা করে লেখা** শব্দগুলোর অর্থ এই তালিকায় দেওয়া হলো।

সাইবার

সাইবার অর্থ হলো ইন্টারনেটের সাথে সম্পর্কিত।

সাইবার অপরাধ

সাইবার অপরাধ হলো যখন অপরাধীরা তাদের অপরাধের জন্য ইন্টারনেট ব্যবহার করে।

যেমন, তারা নিম্নোক্ত কাজগুলো করতে ইন্টারনেট ব্যবহার করতে পারে:

- আপনার ব্যক্তিগত তথ্য চুরি করা
- আপনার অনলাইন অ্যাকাউন্ট বা প্রোফাইলের দখল নিয়ে নেওয়া।

লোকেশন সেটিংস

আপনার ডিভাইস কোথায় আছে যা দেখা যায় লোকেশন সেটিংস এর মাধ্যমে।

মাল্টি ফ্যাক্টর অথেনটিকেশন (এমএফএ)

অ্যাকাউন্টে প্রত্যেকবার লগ ইন করার সময় ২ বা ততোধিক ভাবে লগ ইন করাকে এমএফএ বলে।

পাসফ্রেজ

পাসওয়ার্ড এর আরও শক্ত ধরনই হলো পাসফ্রেজ।

এটি অন্য কারও অনুমান করা খুবই কঠিন।

পাবলিক ওয়াই-ফাই

পাবলিক জায়গায় ব্যবহারের জন্যে দেওয়া ফ্রি ওয়ারলেস ইন্টারনেটকে বলে পাবলিক ওয়াই-ফাই।

প্রতারণা

কেউ যদি নিচের কাজগুলো করার চেষ্টা করে তাকে আমরা প্রতারণা (scam) বলি:

- আপনাকে ঠকানো
- আপনার টাকা নেওয়া।

প্রতারক

যারা প্রতারণা করে তাকে আমরা প্রতারক (scammer) বলি।

আমাদের সাথে যোগাযোগ করুন

আপনি অস্ট্রেলিয়ান সাইবার সিকিউরিটি হটলাইনে ফোন করতে পারেন।

1300 292 371

আপনি আমাদের ওয়েবসাইটে যেতে পারেন।
www.actnowstaysecure.gov.au

আপনি ReportCyber এর ওয়েবসাইটে কোনো সাইবার অপরাধ রিপোর্ট করতে পারেন।

www.cyber.gov.au/report

এই সহজে পড়ার নথিটি স্টক ছবি ও নিজস্ব ছবি ব্যবহার করে তৈরি করেছে ইনফরমেশন এক্সেস গ্রুপ। অনুমতি ছাড়া এই ছবিগুলো ব্যবহার করা যাবে না। ছবিগুলো সম্পর্কে কোনো প্রশ্ন থাকলে এই ওয়েবসাইটে যান: www.informationaccessgroup.com. কাজের নাম্বার (Job number) ৬৩৪২ উল্লেখ করুন।