

নয়টি অপরিহার্য সাইবার নিরাপত্তার অভ্যাস আজকে গ্রহণ করুন



1. আপনি ক্লিক করার আগে বিরতি দিন!

লিঙ্কে ক্লিক করার আগে দুবার চিন্তা করুন যাতে সংযুক্তিগুলি রোপেন করা যায়, এমনকি যদি সেগুলি আপনার পরিচিত কারো কাছ থেকে এসেছে বলে মনে হয়।

- সর্বদা পরিচিত, বৈধ সাথী উত্সের মাধ্যমে ওয়েবসাইটগুলিতে নেভিগেট করুন (যেমন HTTPS) অজানা লিঙ্কগুলিতে ক্লিক করার পরিবর্তে।
- যদি একটি সংযুক্তি অপ্রত্যাশিত মনে হয়, বিশ্বস্ত পদ্ধতির মাধ্যমে প্রেরকের সাথে নিশ্চিত করুন বা নিরাপদে থাকার জন্য ক্লিক না করা বেছে নিন।



2. ব্যক্তিগত তথ্যের জন্য অনুরোধ যাচাই করুন

সর্বদা ব্যক্তিগত ডেটার জন্য অনুরোধগুলি নিশ্চিত করুন—সেটি আপনার বা অন্য কারও।

- স্ক্যামাররা সহজেই বিশ্বস্ত পরিচিতিদের ছদ্মবেশ ধারণ করতে পারে।
- অস্বাভাবিক কার্যকলাপের জন্য নিয়মিত আর্থিক বিবৃতি এবং ক্রেডিট রিপোর্ট পর্যালোচনা করুন।
- অনেক ফিশিং বার্তায় বানান এবং ব্যাকরণগত ত্রুটি রয়েছে।
- অনুরোধটি বৈধ কিনা তা বিবেচনা করুন। ব্যক্তি বা প্রতিষ্ঠানের কি সেই তথ্যের প্রয়োজন আছে



3. আপনার পাসওয়ার্ড নিয়ন্ত্রণ করুন

আপনার অ্যাকাউন্ট সুরক্ষিত রাখার জন্য শক্তিশালী, জটিল পাসওয়ার্ড তৈরি করা এবং সেগুলিকে বুদ্ধিমানের সাথে পরিচালনা করা অপরিহার্য।

- বিভিন্ন অ্যাকাউন্টের জন্য অনন্য পাসওয়ার্ড ব্যবহার করুন।
- কর্ম এবং ব্যক্তিগত পাসওয়ার্ড আলাদা রাখুন।
- কখনোই পাসওয়ার্ড শেয়ার করবেন না।
- ঘন ঘন পাসওয়ার্ড পরিবর্তন করুন।
- ব্রাউজারে পাসওয়ার্ড সেভ করা বন্ধ করুন।
- অতিরিক্ত নিরাপত্তার জন্য মাল্টি-ফ্যাক্টর প্রমাণীকরণ (MFA) সক্ষম করুন।



4. আপনার ডিভাইস সুরক্ষিত

আপনার কাজের জায়গা লকআপ করুন এবং দূরে যাওয়ার সময় আপনার ডিভাইসগুলিকে সুরক্ষিত করুন

- সর্বদা আপনার কম্পিউটার স্ক্রীন লক করুন।
- আপনার ফোন এবং পোর্টেবল ডিভাইসগুলি আপনার সাথে নিন বা সেগুলিকে নিরাপদে সংরক্ষণ করুন।
- যখনই সম্ভব শক্তিশালী প্রমাণীকরণ পদ্ধতি ব্যবহার করুন।



5. গুরুত্বপূর্ণ ফাইল ব্যাকআপ করুন

নিশ্চিত করুন যে আপনার সমালোচনামূলক ডেটা নিয়মিত ব্যাকআপ আছে।

- মূল থেকে একটি পৃথক অবস্থানে ব্যাকআপ সংরক্ষণ করুন।
- সংস্থা-অনুমোদিত স্টোরেজ সমাধান ব্যবহার করুন।
- সঠিকভাবে ফাংশন নিশ্চিত করতে নিয়মিত সর্বশেষ ব্যাকআপ।



6. সন্দেহজনক কার্যকলাপ রিপোর্ট করুন

যদি কিছু সন্দেহজনক মনে হয়, আপনার প্রবৃত্তি বিশ্বাস করুন - এটি রিপোর্ট করুন!

- সন্দেহভাজন প্রতারক বা সন্দেহজনক কার্যকলাপের জন্য আপনার সুপারভাইজারকে সতর্ক করুন এবং আপনার সংস্থার রিপোর্টিং প্রোটোকল অনুসরণ করুন



7. নিজেকে এবং অন্যদের শিক্ষিত করুন সাম্প্রতিক সাইবার নিরাপত্তা হুমকি এবং প্রবণতা সম্পর্কে অবগত থাকুন।

- প্রশিক্ষণ সেশনে যোগ দিন এবং সুযোগ পেলে সহকর্মীদের সাথে জ্ঞান ভাগ করুন।
- সাইবার হুমকির বিরুদ্ধে আপনার প্রতিরক্ষার প্রথম লাইন হল একটি সুপরিচিত দল।



8. সিকিউর নেটওয়ার্ক ব্যবহার করুন

সর্বদা সুরক্ষিত নেটওয়ার্কের সাথে সংযোগ করুন, বিশেষ করে যখন সংবেদনশীল তথ্য অ্যাক্সেস করা হয়।

- আর্থিক লেনদেন বা সংবেদনশীল কাজের জন্য পাবলিক ওয়াই-ফাই এড়িয়ে চলুন।
- অতিরিক্ত সুরক্ষার জন্য প্রয়োজন হলে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (ভিপিএন) ব্যবহার করুন।



9. সোশ্যাল মিডিয়ার সাথে সতর্ক থাকুন

আপনি অনলাইনে যে ব্যক্তিগত তথ্য শেয়ার করেন তার পরিমাণ সীমিত করুন। তাই আপনি আপনার গোপনীয়তা রক্ষা করতে পারেন, আপনার নিরাপত্তা বাড়াতে পারেন এবং আরও ইতিবাচক অনলাইন অভিজ্ঞতা তৈরি করতে পারেন।

- সোশ্যাল মিডিয়া প্ল্যাটফর্মগুলিতে গোপনীয়তা সেটিংস পর্যালোচনা করুন।
- বন্ধুত্বের অনুরোধ এবং যারা আপনার তথ্য অ্যাক্সেস করেছে তার প্রতি মনোযোগ দিন; একটি লক করা প্রোফাইল থেকে অনুরোধ গ্রহণ করবেন না।
- সম্ভাব্য ঝুঁকি কমাতে নিয়মিতভাবে আপনার অনলাইন উপস্থিতি নিরীক্ষণ করুন।

মনে রাখবেন: সাইবার সিকিউরিটি প্রত্যেকের দায়িত্ব!