আজি গ্রহণ কৰিবলগীয়া ৯টা অত্যাৱশ্যকীয় চাইবাৰ সুৰক্ষাৰ অভ্যাস
Nine Essential Cyber Security Habits to Adopt Today

1. 

ক্লিক কৰাৰ আগতে থমকি ৰওক
Pause Before You Click!

লিংকত ক্লিক কৰাৰ আগতে বা সংলগ্নক খোলাৰ আগতে দুবাৰ ভাবি চাওক, যদিও সেইবোৰ আপোনাৰ চিনাকি কোনোবা এজনৰ পৰা অহা যেন লাগে

Think twice before clicking on links or opening attachments, even if they appear to come from someone you know.

- অজ্ঞাত লিংকত ক্লিক কৰাৰ পৰিৱর্তে সদায় এটা জনা, বৈধ উৎসৰ জৰিয়তে (যেনে HTTPS) ৱেবছাইটসমূহলৈ নেভিগেট কৰক।
- Always navigate to websites through a known, legitimate source (Eg. HTTPS) instead of clicking on unknown links.
- যদি কোনো সংলগ্নক অপ্রত্যাশিত যেন লাগে, এটা বিশ্বাসযোগ্য পদ্ধতিৰ যোগেদি প্রেৰকৰ সৈতে নিশ্চিত কৰক অথবা সুৰক্ষিত থাকিবলৈ ক্লিক কৰাৰ পৰা বিৰত থাকক।
- If an attachment seems unexpected, confirm with the sender via a trusted method or choose not to click, to be on the safer side.

2. ব্যক্তিগত তথ্যৰ বাবে অহা অনুৰোধসমূহ পৰীক্ষা কৰক
Verify Requests for Personal Information

ব্যক্তিগত তথ্যৰ বাবে অহা অনুৰোধসমূহ সদায় নিশ্চিত কৰক—সেয়া আপোনাৰ হওক বা আন কাৰোবাৰ হওক।

Always confirm requests for private data—whether it's yours or someone else's.

- স্কাম্যাৰে সহজেই বিশ্বাসযোগ্য সম্পর্কৰ ছদ্মবেশ ল'ব পাৰে।
- Scammers can easily impersonate trusted contacts.
- অস্বাভাৱিক কার্য্যকলাপৰ বাবে বিত্তীয় বিৱৰণ আৰু ঋণ প্রতিবেদন নিয়মিতভাৱে পর্যালোচনা কৰক।
- Regularly review financial statements and credit reports for unusual activity.
- বহুতো ফিছিং বার্তাত বানান আৰু ব্যাকৰণগত ভুল থাকে।
- Many phishing messages contain spelling and grammatical errors.
- অনুৰোধটো বৈধ নেকি সেই বিষয়ে বিবেচনা কৰক। ব্যক্তি বা সংস্থাটোক সেই তথ্যৰ প্রয়োজন হোৱাৰ সম্ভাৱনা আছেনে?
- Consider whether the request is legitimate. Is the person or organization likely to need that information?

3. আপোনাৰ পাছৱৰ্ডসমূহ নিয়ন্ত্ৰণ কৰক

শক্তিশালী, জটিল পাছৱৰ্ড সৃষ্টি কৰা আৰু বুদ্ধিমানৰূপে পৰিচালনা কৰাটো আপোনাৰ একাউণ্টসমূহ সুৰক্ষিত ৰখাৰ বাবে অতি প্ৰয়োজনীয়।

Control Your Passwords

Creating strong, complex passwords and managing them wisely is essential for keeping your accounts secure.

- বিভিন্ন একাউণ্টৰ বাবে অনন্য পাছৱৰ্ড ব্যৱহাৰ কৰক।
  Use unique passwords for different accounts.
- কাম আৰু ব্যক্তিগত পাছৱৰ্ড পৃথক ৰাখক।
  Keep work and personal passwords separate.
- কেতিয়াও পাছৱৰ্ড শ্বেয়াৰ নকৰিব।
  Never share passwords.
- সঘনাই পাছৱৰ্ড সলনি কৰক।
  Change password frequently.
- ব্ৰাউজাৰত পাছৱৰ্ড সংৰক্ষণ কৰাৰ পৰা আঁতৰি থাকক।
  Opt out of saving passwords in browsers.
- অতিৰিক্ত সুৰক্ষাৰ বাবে বহু-কাৰক প্ৰমাণীকৰণ (MFA) সামৰ্থবান কৰক।
  Enable multi-factor authentication (MFA) for added security.

4. আপোনাৰ ডিভাইচসমূহ সুৰক্ষিত কৰক
Secure Your Devices

আপোনাৰ কাৰ্য্যস্থান লক আপ কৰক আৰু আঁতৰি যোৱাৰ সময়ত আপোনাৰ ডিভাইচসমূহ সুৰক্ষিত কৰক।

Lock up your workspace and protect your devices when stepping away.

- আপোনাৰ কম্পিউটাৰৰ পৰ্দা সদায় লক কৰক।

Always lock your computer screen.

- আপোনাৰ ফোন আৰু পৰ্টেবল ডিভাইচসমূহ আপোনাৰ লগত লৈ যাওক অথবা সুৰক্ষিতভাৱে সংৰক্ষণ কৰক।

Take your phone and portable devices with you or store them securely.

- সম্ভৱ হ'লে শক্তিশালী প্ৰমাণীকৰণ পদ্ধতি ব্যৱহাৰ কৰক।

Utilize strong authentication methods whenever possible.

5. গুৰুত্বপূৰ্ণ ফাইলসমূহৰ বেকআপ লওক।

Backup Important Files

আপোনাৰ জটিল তথ্য নিয়মিতভাৱে বেকআপ লোৱাটো নিশ্চিত কৰক।

Ensure that your critical data is backed up regularly.

- বেকআপসমূহ মূলস্থানৰ পৰা এটা পৃথক স্থানত সংৰক্ষণ কৰক।

Store backups in a separate location from originals.

- সংস্থা-অনুমোদিত সংৰক্ষণ সমাধান ব্যৱহাৰ কৰক।

Use organization-approved storage solutions.

- বেকআপসমূহ সঠিকভাৱে কাম কৰাটো নিশ্চিত কৰিবলৈ নিয়মিতভাৱে পৰীক্ষা কৰক।

Regularly test backups to ensure they function properly.

6. সন্দেহজনক কার্য্যকলাপৰ ৰিপৰ্ট কৰক

Report Suspicious Activity

যদি কিবা এটা সন্দেহজনক যেন লাগে, তেন্তে আপোনাৰ প্ৰবৃত্তিক বিশ্বাস কৰক—ৰিপ'ৰ্ট কৰক!

If something seems suspicious, trust your instincts—report it!

- আপোনাৰ তত্বাৱধায়কক সতর্ক কৰক আৰু সন্দেহযুক্ত কেলেংকাৰী বা সন্দেহজনক কার্য্যকলাপৰ বাবে আপোনাৰ প্ৰতিষ্ঠানৰ প্ৰতিবেদন প্ৰট'কল অনুসৰণ কৰক৷

Alert your supervisor and follow your organization's reporting protocol for suspected scams or suspicious activities.

7.নিজৰ লগতে আনকো শিক্ষিত কৰক

Educate Yourself and Others

শেহতীয়া চাইবাৰ সুৰক্ষাৰ ভাবুকি আৰু ধাৰাসমূহৰ বিষয়ে অৱগত থাকক।

Stay informed about the latest cyber security threats and trends.

- প্ৰশিক্ষণ অধিবেশনত অংশগ্ৰহণ কৰক আৰু সুযোগ পালেই সহকর্মীসকলৰ সৈতে জ্ঞান ভাগ-বতৰা কৰক।

Attend training sessions and share knowledge with colleagues as and when you get an opportunity.

- এটা সু-অৱগত দল হৈছে চাইবাৰ ভাবুকিৰ বিৰুদ্ধে আপোনাৰ প্ৰথম প্ৰতিৰক্ষা লাইন।

A well-informed team is your first line of defence against cyber threats.

8. **সুৰক্ষিত নে'টৱৰ্কসমূহ ব্যৱহাৰ কৰক**

Use Secure Networks

সদায় সুৰক্ষিত নে'টৱৰ্কসমূহৰ সৈতে সংযোগ কৰক, বিশেষকৈ স্পৰ্শকাতৰ তথ্য প্ৰাপ্ত কৰাৰ সময়ত।

Always connect to secure networks, especially when accessing sensitive information.

- বিত্তীয় লেনদেন বা স্পৰ্শকাতৰ কামৰ বাবে ৰাজহুৱা ৱাই-ফাই ব্যৱহাৰ কৰাৰ পৰা বিৰত থাকক।

Avoid public Wi-Fi for financial transactions or sensitive work.

- অধিক সুৰক্ষাৰ বাবে প্ৰয়োজন হ'লে এটা ভাৰ্চুৱেল ব্যক্তিগত নে'টৱৰ্ক (VPN) ব্যৱহাৰ কৰক।

Use a Virtual Private Network (VPN) when necessary for added protection.

9. ছ'চিয়েল মিডিয়াৰ সৈতে সাৱধান হওক

Be Cautious with social media

আপুনি অনলাইনত শ্বেয়াৰ কৰা ব্যক্তিগত তথ্যৰ পৰিমাণ সীমিত কৰক।

Limit the amount of personal information you share online.

গতিকে আপুনি আপোনাৰ গোপনীয়তা সুৰক্ষিত কৰিব পাৰে, আপোনাৰ সুৰক্ষা বৃদ্ধি কৰিব পাৰে, আৰু অধিক ইতিবাচক অনলাইন অভিজ্ঞতা সৃষ্টি কৰিব পাৰে।

So you can protect your privacy, enhance your safety, and create a more positive online experience.

- ছ'চিয়েল মিডিয়া প্লেটফৰ্মত গোপনীয়তা ছেটিংছ পৰ্যালোচনা কৰা।

Review privacy settings on social media platforms.

- বন্ধুৰ অনুৰোধ আৰু আপোনাৰ তথ্য কোনে লাভ কৰিব পাৰে সেই বিষয়ে সচেতন হওক; এটা লক কৰা প্ৰফাইলৰ পৰা অনুৰোধ গ্ৰহণ নকৰিব।

Be mindful of friend requests and who has access to your information; do not accept requests from a locked profile.

- সম্ভাৱ্য বিপদ কম কৰিবলৈ আপোনাৰ অনলাইন উপস্থিতি নিয়মিতভাৱে অডিট কৰক।

Regularly audit your online presence to minimize potential risks.

মনত ৰাখিব: চাইবাৰ সুৰক্ষা সকলোৰে দায়িত্ব!

Remember: Cyber Security is Everyone's Responsibility!