ICT DIVISION
FUTURE IS HERE

Digital Security Agency

কোভিড-১৯ মহামারি চলাকালীন ডিজিটাল হাইজিন

ডিজিটাল নিরাপত্তা এজেন্সি
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ
আইসিটি টাওয়ার, আগারগাঁও, ঢাকা
dsa.gov.bd

সূচিপত্র

কোভিড-১৯ মহামারি চলাকালীন ডিজিটাল হাইজিন

১.০ ভূমিকা:

বিশ্বব্যাপী ছড়িয়ে পড়া কোভিড-১৯ ভাইরাস বিস্তারের কারণে প্রতিনিয়ত দেশে ইন্টারনেট ব্যবহার বৃদ্ধি পাচ্ছে। ইন্টারনেট ব্যবহার বৃদ্ধির সাথে সাথে ডিজিটাল সুরক্ষায় ঝুঁকি বাড়ছে। বর্তমান সময়ে করোনাভাইরাস সম্পর্কিত স্ক্যাম এবং ফিশিং প্রচারগুলি বাড়ছে। বিশ্ব এখন মহামারি কোভিড-১৯ ব্যবস্থাপনায় ব্যস্ত। এ সম্পর্কিত রোগের লক্ষণ, রোগের প্রতিকার, প্রতিষেধক এবং অন্যান্য বিষয় সম্পর্কে মানুষ ইন্টারনেটে তথ্য খুঁজতে আগ্রহী হচ্ছে। এ সময়ে সাইবার অপরাধীরা জনগণের ভয় ও আগ্রহকে তাদের সুবিধার্থে ব্যবহার করছে, নতুন নতুন জালিয়াতি এবং অভিনব কায়দা তৈরি করছে এবং ব্যক্তি, সংস্থা এমনকি পুরো শিল্পকে লক্ষ্যবস্তু করছে। ফলে এ সকল বিষয়ে সচেতনতা এবং সর্তকতা অবলম্বন করা জরুরি। ডিজিটাল প্লাটফরমে নিজেকে সুরক্ষিত রাখার জন্য নিম্নবর্ণিত বিষয়গুলি অনুসরণ করা যেতে পারে।

১.১ ডিজিটাল ডিভাইস ব্যবহারের ক্ষেত্রে ব্যবহারকারীদের করণীয়:

মহামারি কোভিড-১৯ এর প্রাদূর্ভাবে বেশিরভাগ প্রতিষ্ঠানই বন্ধ রয়েছে। এ সময়ে অধিকাংশ কর্মকর্তা/কর্মচারী এখন বাড়ী থেকে কাজ করছে। home-user রা সাধারণত সর্বদা এন্টারপ্রাইজ নেটওয়ার্কের সুরক্ষা ব্যবস্থার সুবিধা নাও পেতে পারে। কিছু ব্যবহারকারী বাড়ীতে তাদের ব্যক্তিগত ডিভাইস/সিস্টেমগুলি ব্যবহার করছেন যেগুলিতে কর্মক্ষেত্রে ব্যবহৃত ডিভাইসগুলির ন্যায় একই স্তরের সুরক্ষা ব্যবস্থা নাও থাকতে পারে। সে লক্ষ্যে সাধারণ ব্যবহারকারী এবং home-user দের জন্য নিম্নবর্ণিত করণীয়সমূহ অনুসরণ করা যেতে পারে:

১.১.১ সাধারণ ব্যবহারকারীদের করণীয় (ই-মেইল এবং ওয়েব অ্যাপ্লিকেশন সংক্রান্ত):

- **Unexpected or unsolicited emails** (অপ্রত্যাশিত বা অযাচিত ইমেল):- বিষয় সম্পর্কিত যে ইমেইল ব্যবহারকারী রিসিভ করেছে যা তার প্রত্যাশিত নয়, সে সম্পর্কে সতর্ক থাকতে হবে - এমনকি পরিচিত ব্যক্তি বা সংস্থা থেকে হলেও।

- **Uses odd email addresses** (অসংগতিপূর্ণ ইমেইল ঠিকানা):- যেসব ইমেইল সংশ্লিষ্ট প্রতিষ্ঠানের নামের সাথে অসংগতিপূর্ণ বা ভুল বানান বা ব্যাকরণ ত্রুটি, অসামঞ্জস্য অভিবাদন- অসংগতিপূর্ণ সন্দেহযুক্ত টেক্সট) রয়েছে, তা আমলে না নেওয়া;

- **Emails stressing urgency** (অতীব জরুরী/এক্ষণি):- বিশেষত যারা নতুন মহামারী সংক্রান্ত তথ্য/বিশ্লেষণ ঘোষণা করে এবং ব্যবহাকারীকে কোন লিঙ্কে ক্লিক করতে বা সাবস্ক্রাইব করার জন্য ব্যক্তিগত তথ্য সরবরাহ করতে বলে এ জাতীয় ইমেইলসমূহ আমলে না নিয়ে সতর্ক থাকতে হবে;

- **Contains attachments** (সংযুক্তি):- ইমেইলের সাথে সংযুক্তিগুলি যদি প্রত্যাশিত না হয় তবে সংযুক্তিগুলি খোলা যাবে না। যদি সন্দেহ হয় এবং প্রেরক বন্ধু বা সহকর্মী হয় তবে এটিকে খোলার আগে যাচাই করার জন্য তাদের সাথে প্রথম যোগাযোগ করা যেতে পারে। সংযুক্তি আসলে প্রকৃত প্রেরকের কাছে থেকে এসেছে কিনা তা নিশ্চিত হওয়া প্রয়োজন;

- **Embedded links** (এম্বেড করা লিংক):- সংযুক্ত বা জুড়ে দেওয়া লিংক থেকে সতর্ক থাকতে হবে। 'বিজ্ঞাপন দেওয়া' ঠিকানা প্রদত্ত লিঙ্কটির সাথে মেলে কিনা তা দেখার জন্য ব্যবহারকারীর মাউসটিকে লিংকের উপরে ঘুরিয়ে দেখা যেতে পারে। তবে নিরাপদ বিকল্প হচ্ছে উদ্ধৃত সংস্থার অফিশিয়াল ওয়েবসাইটে স্বাধীনভাবে নেভিগেট করা এবং ইমেলের লিংক ব্যবহার না করা। এমনকি ব্যবহারকারী যদি কোন malicious লিংকে ক্লিক করে এবং "404 ERROR – WEBSITE NOT FOUND" নোটিশও পেয়ে থাকে তবুও ব্যবহারকারী ডিভাইস আক্রমণের শিকার হতে পারে;

- **Fake information** (মিথ্যা সংবাদ বা তথ্য):- মিথ্যা সংবাদ বা তথ্য সম্পর্কে সচেতন থাকতে হবে। শুধুমাত্র ভেরিভাইড উৎস থেকে প্রাপ্ত তথ্যকে বিশ্বাস করতে হবে;

- **Provide sensitive information** (সংবেদনশীল তথ্য প্রদান):- সংবেদনশীল তথ্য প্রদানের জন্য অনুরোধগুলি সম্পর্কে সতর্ক হওয়া - যেমন ব্যবহারকারীর নাম, পাসওয়ার্ড বা ক্রেডিট কার্ডের বিবরণ। সাধারণত: সেবা দানকারী কোন প্রতিষ্ঠান ই-মেইলে/ফোনে কখনই এই জাতীয় তথ্য জিজ্ঞাসা করবে না এবং তারা কখনও আপনার পাসওয়ার্ড বা পিন জানতে চায় না;
- **Browser and plugins** (ব্রাউজার এবং প্লাগইন):-সাধারণত ওয়েব ব্রাউজারসমূহ ইন্টারনেট যোগাযোগের প্রথম পয়েন্ট হিসেবে কাজ করে। ব্রাউজারের নিরাপত্তা নিশ্চিত করতে ডেভেলপারগণ ঘন ঘন আপডেট প্রকাশ করে, তাই ব্রাউজার এবং প্রয়োজনীয় প্লাগইনসমূহ নিয়মিত আপডেট রাখা জরুরি;
- **Block Pop-ups (**পপ-আপ ব্লক) সাধারণ ব্যবহারকারী হিসেবে ব্রাউজারে পপ-আপ দেখলেই ক্লিক না করা। ব্রাউজার পপ-আপগুলি সাধারণত বিজ্ঞাপন প্রচারের জন্য নতুন ব্রাউজার উইন্ডো ওপেন করে এবং বেশিরভাগই কেবল বিরক্তিকর এবং malicious বা অনুপযুক্ত কন্টেন্ট থাকতে পারে;
- **Clear cookies** (কুকিজ ক্লিয়ার রাখা):- অযাচিত কুকিজ নিয়মিত ডিলিট করা প্রয়োজন; কুকিজে সাধারণত ব্যবহারকারীর বিভিন্ন তথ্য থাকে যেমন- নির্দিষ্ট কোন ওয়েবসাইটে ব্যবহারকারীর পছন্দের তালিকা;
- **Avoid torrenting sites** (টরেন্টিং সাইট পরিহার করা):- ফাইল শেয়ারিং সাইট এবং টরেন্টিং সাইটসমূহ পরিহার করা উচিৎ। এসকল সাইট অন্যান্য ব্যবহারকারীদের সাথে ফাইল শেয়ার করতে পারে;
- **Download** (ডাউনেলোড):- প্রয়োজনীয় কোন সফটওয়্যার, অ্যাপ বা অডিও/ভিডিও শুধুমাত্র ট্রাস্টেড সাইট/স্টোর থেকে ডাউনলোড করা;
- **Logout** (লগ আউট):-নিরাপদ কোন সাইটে কার্যসম্পাদন শেষে অবশ্যই লগ আউট করা;
- সরকারি ইমেইল নীতিমালা ২০১৮ অনুসরণ করা।

১.১.২ Home-User (বাড়ি থেকে ব্যবহারকারী)-দের করণীয়:

অধিকাংশ কর্মকর্তা/কর্মচারী এখন বাড়ি থেকে কাজ করছে। বিদ্যমান পরিস্থিতিতে ডিজিটাল বিশ্বে বাড়ি থেকে ব্যবহারকারীদের অতিরিক্ত ঝুঁকি সৃষ্টি করতে পারে। এ পরিস্থিতিতে নিম্নলিখিত বিষয়সমূহ সেই ঝুঁকিগুলি হ্রাস করতে সহায়তা করে:

- প্রতিষ্ঠান কর্তৃক প্রদত্ত ল্যাপটপ ব্যবহার করা (যদি সম্ভব হয়)- এটি ব্যক্তিগত কম্পিউটারের চেয়ে আরও শক্তিশালী সুরক্ষা প্রদান করবে;
- ডিভাইসটি সবসময় আপডেট রাখা- অপারেটিং সিস্টেমসহ যে সমস্ত সফ্টওয়্যার, সুরক্ষা আপডেট, অ্যান্টি-ম্যালওয়্যার এবং প্যাচগুলি প্রয়োগ করা হয়েছে তা আপ-টু-ডেট রয়েছে মর্মে নিশ্চিত থাকতে হবে;
- প্রাতিষ্ঠানিক কাজের সাথে সংযোগের জন্য অনুমোদিত সুরক্ষিত রিমোট অ্যাক্সেস সংযোগ ব্যবহার করা প্রয়োজন (যদি সম্ভব হয়)- এই সংযোগগুলির বেশিরভাগই একটি এনক্রিপ্টেড পয়েন্ট-টু-পয়েন্ট ভিপিএন সেশন সরবরাহ করে;
- সর্বদা জটিল Passphrases/Password ব্যবহার করা;
- রিমোট অ্যাকসেস সেশনে সংযুক্ত থাকাকালীন সময়ে ব্যক্তিগত কারণে ওয়েব ব্রাউজ না করা-এটি রিমোট সংযোগে স্থাপিত নেটওয়ার্ককে সংক্রমন ঘঠাতে পারে;
- সুরক্ষা সিস্টেমগুলি যেমন-অ্যান্টি-ম্যালওয়্যার বা ফায়ারওয়াল Disable না করা;
- পাবলিক ওয়াই-ফাই ব্যবহার করে কাজ পরিচালনা করা পরিহার করা;
- কম্পিউটার/ল্যাপটপ idle অবস্থায় রিমোট সংযোগ বন্ধ রাখা এবং স্ক্রীনটিকে লক রাখা;
- পরিবারের সদস্য বা অন্য কাউকে প্রতিষ্ঠান কৃর্তক সরবরাহকৃত ডিভাইস ব্যবহারের অনুমতি না দেওয়া;
- পরিবারের সদস্যদের সাথে পাসওয়ার্ড শেয়ার না করা;

- Shared Device এ পাসওয়ার্ড সংরক্ষণ না করা;
- Two-Factor Authentication এনাবল রাখা- Two-Factor Authentication ব্যক্তিগত তথ্যের সুরক্ষায় একটি অতিরিক্ত প্রতিরক্ষা স্তর নিশ্চিত করে। ব্যক্তিগত এবং দাপ্তরিক অ্যাকাউন্টগুলির জন্য সর্বদা Two-Factor Authentication অথেনটিকেশন ব্যবহার করা;
- মাল্টিফাংশনাল ডিভাইস যেমন: ফটোকপিয়ার ব্যবহারের ক্ষেত্রে সর্তকতা অবলম্বন করা (গুরুত্বপূর্ণ তথ্যাদি ফটোকপিয়ারের মেমরিতে সংরক্ষিত থাকতে পারে);
- রিমুভল ড্রাইভ স্ক্যান না করে ব্যবহার করা থেকে বিরত থাকা;
- পিসি স্পীড বুস্টার বা র‍্যাম ক্লিনার ব্যবহার থেকে বিরত থাকা;

২.০ সামাজিক যোগাযোগ মাধ্যম ব্যবহারের সতর্কতা:

সামাজিক যোগাযোগ মাধ্যম ব্যবহারে যেমন উপকারিতা রয়েছে তেমনি অসর্তকতার কারণে অনেক ক্ষেত্রে ব্যবহারকারীদের ভোগান্তিতেও পড়তে হয়ে। গুজবের অনেক ঘটনা সামাজিক যোগাযোগের মাধ্যমে বেশি ঘটছে। আর ব্যবহারকারীরর অ্যাকাউন্টটি যদি হ্যাকড হয়ে যায় সে ক্ষেত্রে জটিলতার শেষ নেই। কোভিড-১৯ প্রাদুর্ভাবে সামাজিক যোগাযোগ মাধ্যমে অনেক মিথ্যা এবং ভূয়া তথ্য ছড়ানো হচ্ছে। ব্যবহারকারীদের আগ্রহকে কাজে লাগিয়ে সাইবার অপরাধীরা সামাজিক যোগাযোগ মাধ্যমেও বিভিন্ন অপরাধ এবং জালিয়াতির আশ্রয় নিচ্ছে। সে লক্ষ্যে সার্বক্ষণিকভাবে সামাজিক যোগাযোগের যেকোনো মাধ্যম ব্যবহারের ক্ষেত্রে সতর্ক থাকতে হবে। কোনটি গুজব আর কোনটি সত্য তা বোঝার পাশাপাশি ব্যক্তিগত এবং প্রাতিষ্ঠানিক অ্যাকাউন্টটি যাতে নিরাপদ থাকে সেই বিষয়েও সাবধানতা অবলম্বন করা জরুরি। এ ক্ষেত্রে সাধারণ ব্যবহারকারীরা নিম্নোক্ত বিষয়সমূহ অনুসরণ করতে পারে:

- সরকারি প্রতিষ্ঠানে সামাজিক যোগাযোগ মাধ্যম ব্যবহার নির্দেশিকা ২০১৯ অনুসরণ করা;
- সামাজিক যোগাযোগ মাধ্যমে অপরিচিত ব্যক্তির ফ্রেন্ড রিকুয়েস্ট গ্রহণ করা থেকে বিরত থাকা;
- প্রাইভেসি সেটিংস যথাযথভাবে সেট করা এবং নিয়মিত পরীক্ষা করা;
- যে কোন পোস্টের ভিউয়ার সঠিকভাবে নির্বাচন করা;
- ফ্রেন্ডলিস্ট অর্গানাইজ করা;
- সামাজিক যোগাযোগ মাধ্যমে প্রতিষ্ঠানের পূর্বানুমোদন ব্যতীত কোন তথ্য বা অভিযোগ শেয়ার করা থেকে বিরত থাকা;
- একাউন্ট হ্যাকড হওয়া থেকে রক্ষা পেতে শক্তিশালী পাসওয়ার্ড ব্যবহার করা;
- লগ-ইন এর ক্ষেত্রে Two-Factor Authentication চালু রাখা;
- দীর্ঘ দিন একই পাসওয়ার্ড ব্যবহার না করা;
- ভিন্ন ভিন্ন সোস্যাল মিডিয়ার একাউন্টে ভিন্ন ভিন্ন পাসওয়ার্ড ব্যবহার করা;
- কোন পোস্টের ট্যাগিং অপশনে ব্যবহারকারীর অনুমোদনের বিষয়টি নিশ্চত করা;
- কোন পোস্টে লাইক, কমেন্ট ইত্যাদির বিষয়ে সর্তকতা অবলম্বন করা;
- ব্যক্তিগত তথ্যাদি গোপন রাখা;
- অন্য ডিভাইসে নিজ একাউন্ট ব্যবহার শেষে আইডি লগ আউট করা;
- বিভিন্ন মোবাইল এপ্লিকেশন ব্যবহারে সর্তক থাকা;
- সোস্যাল মিডিয়ায় একাউন্ট পরিচালনায় আপডেটেড ব্রাউজার/অ্যাপস ব্যবহার করা;
- সোস্যাল মিডিয়ায় প্রকাশিত যে কোন তথ্যের ভিত্তিতে কোন কার্যক্রম গ্রহণ করার পূর্বে তার উৎস/সঠিকতা যাচাই করা;
- “সত্য-মিথ্যা যাচাই আগে, ইন্টারনেটে শেয়ার পরে” এই স্লোগানটির ভিত্তিতে সামাজিক যোগাযোগ মাধ্যমে কোন কিছু শেয়ার করার আগে যাচাই করা।

৩.০ স্মার্টফোন ব্যবহারে সতর্কতা:

বর্তমান তথ্যপ্রযুক্তির যুগে স্মার্টফোন প্রতিদিনের সঙ্গী। এটি ছাড়া আমাদের এক মুহূর্তও চলে না। স্মার্টফোনের নিরাপত্তার বিষয়টিও এখন গুরুত্বপূর্ণ। ডেস্কটপ কিংবা ল্যাপটপের ইন্টারনেটভিত্তিক অনেক কাজই এখন মানুষ স্মার্টফোনে সম্পন্ন করে থাকে। স্মার্ট ফোনে ইন্টারনেট ব্যবহারের ফলে সাইবার অপরাধীরাও বেশ সক্রিয়। ফলে সতর্কতা অবলম্বন না করলে সাইবার অপরাধীরা খুব সহজেই তাদের উদ্দেশ্য পূরণ করতে পারে। এ বিষয়ে নিম্নোক্ত বিষয়সমূহ অনুসরণ করা উচিত:

- ডিভাইসে শক্তিশালী এবং জটিল পাসওয়ার্ড বা বায়োমেট্রিক অথেনটিকেশন ব্যবহার করা। পাসওয়ার্ড নির্ধরণ করার ক্ষেত্রে ফোন নম্বর, জন্ম-তারিখ ইত্যাদি ব্যবহার না করা;
- Anti-Theft Feature ব্যবহার করা- এতে হারিয়ে যাওয়া ফোনটি খুজঁতে সহজতর হয়;
- অপারেটিং সিস্টেম এবং ব্যবহৃত অ্যাপসমূহ নিয়মিত আপডেট রাখা;
- ভেরিভাইড স্টোর (গুগল প্লে স্টোর, অ্যাপলের অ্যাপস্টোর ইত্যাদি) থেকে এপস ইন্সটল করা;
- এপস ইন্সটলের সময় ফোনের ক্যামেরা, কন্ট্যাক্ট, গ্যালারি ইত্যাদি অনুমতির বিষয়ে সর্তক থাকা;
- পাবলিক ওয়াই-ফাই এবং হটস্পট ব্যবহার করে আর্থিক লেনদেন, দাপ্তরিক কার্যক্রম কিংবা গোপনীয় কার্যক্রম পরিচালনা না করা;
- ডিভাইস ট্রাকিং চালু রাখা;
- অপ্রয়োজনে ব্লু-টুথ বা লোকেশন সার্ভিস অন না রাখা;
- অপরিচিত ব্যক্তিকে নিজের স্মার্টফোন ব্যবহার করতে দেওয়া থেকে বিরত থাকা;
- স্প্যাম কল বা লিংকে ক্লিক করা থেকে বিরত থাকা;
- গুরুত্বপূর্ণ তথ্যাদি এনক্রিপ্টেড অবস্থায় রাখা;
- স্মার্ট ফোনে অপরিচিত মেসেজের রিপ্লাই বা লোভনীয় অফারের বিষয়সমূহ এড়িয়ে চলা;
- ভেরিফাইড/ট্রাস্টেড এন্টি-ম্যালওয়্যার অ্যাপ ব্যবহার করা।

৪.০ ডিভাইসে সাইবার আক্রমণ/ম্যালওয়্যার আক্রমণের সাধারণ লক্ষণসমূহ:

আক্রমণকারীর দক্ষতার উপর নির্ভর করে কখনও কখনও ব্যবহারকারী আক্রমণের লক্ষণসমূহ দেখতে পায় না। কিছু ক্ষেত্রে নিম্নলিখিত সাধারণ লক্ষণগুলি পরিলক্ষিত হয়:

- পপ-আপ উইন্ডোগুলি স্বয়ংক্রিয়ভাবে ওপেন হওয়া যা পূর্বে ছিল না;
- ব্রাউজারের হোমপেজের পরিবর্তন;
- ব্রাউজারে স্বয়ংক্রিয়ভাবে কোন টুলবার যুক্ত হওয়া;
- অপ্রত্যাশিত সিস্টেম এবং অ্যাপ্লিকেশন আচরণ এবং /অথবা সিস্টেম ক্র্যাশ;
- অজানা প্রোগ্রামসমূহ সিস্টেমে চালিত হওয়া;
- অ্যান্টি-ম্যালওয়্যার স্বয়ংক্রিয়ভাবে Disable হয়ে যাওয়া;
- কম্পিউটার কর্মক্ষমতা ধীর হয়ে যাওয়া;
- অননুমোদিত পাসওয়ার্ড পরিবর্তন অথবা পাসওয়ার্ড পরিবর্তন বা Validation এর জন্য অপ্রত্যাশিত অনুরোধ;
- ফাইল/ফোল্ডার বা স্টোরেজ ড্রাইভ এনক্রিপ্টেড হয়ে যাওয়া বা খুলতে না পারা;
- অপ্রত্যাশিত ফাইল ডিলিট বা কনটেন্টের পরিবর্তন;
- ইন্টারনেট সার্চসমূহ Redirected হওয়া;
- অজানা এন্টি-ভাইরাস সফটওয়্যার স্বয়ংক্রিয়ভাবে স্ক্যানিং শুরু হওয়া;

৫.০ ডিভাইসে সাইবার আক্রমণ/ম্যালওয়্যার আক্রমণ হলে তাৎক্ষণিক করণীয়:

- ডিভাইসটিকে ইন্টারনেটসহ সব ধরণের নেটওয়ার্ক থেকে সংযোগ বিচ্ছিন্ন করা;
- যে কোন প্রকার রিমোট অ্যাক্সেস সেশনের সংযোগ বিচ্ছিন্ন করা;

- ডিভাইসটি বন্ধ করা;
- সন্দেহজনক কার্যক্রম লিপিবদ্ধ করা;
- সেবা প্রদানকারী বা প্রতিষ্ঠানের নিরাপত্তা শাখার সাথে যোগাযোগ করা।

৬.০ উপসংহার:

সাইবার নিরাপত্তার হুমকি ক্রমবর্ধমান ডিজিটাইজেশন এবং নতুন প্রযুক্তির সাথে পরিবর্তিত হচ্ছে। বর্তমান কোভিড-১৯ পরিস্থিতিতে সাইবার অপরাধীরা বেশ সক্রিয়। ডিজিটাল ডিভাইস ব্যবহারকারীদের এ মহামারীর সময়সহ সাবক্ষণিক উল্লিখিত করণীয়সমূহ অনুসরণ করা উচিৎ। সাধারণ ব্যবহারকারীদের ডিজিটাল নিরাপত্তার প্রাথমিক বিষয়সমূহের উপর প্রশিক্ষণ গ্রহণ করে আপডেটেড থাকা প্রয়োজন। ব্যবহারকারীরর সচেতনতাই সাইবার আক্রমণের বিরুদ্ধে সেরা প্রতিরক্ষা।