গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
খাদ্য অধিদপ্তর
কম্পিউটার নেটওয়ার্ক ইউনিট
১৬, আব্দুল গণি রোড, ঢাকা-১০০০
https://dgfood.gov.bd

স্মারক নম্বর: ১৩.০১.০০০০.০০০.১০০.৩১.০০২৩.২১.৭৪

তারিখ: ১১ চৈত্র ১৪৩২ বঙ্গাব্দ
২৫ মার্চ ২০২৬ খ্রিস্টাব্দ

বিষয়: অনলাইন ও সামাজিক যোগাযোগ মাধ্যমে প্রতারণার শিকার হওয়া থেকে সুরক্ষা পেতে প্রয়োজনীয় দিক-নির্দেশনা

উপর্যুক্ত বিষয়ের পরিপ্রেক্ষিতে জানানো যাচ্ছে যে, সম্প্রতি একটি সংঘবদ্ধ প্রতারক চক্র মহাপরিচালক (খাদ্য অধিদপ্তর) মহোদয়ের নাম ও ছবি ব্যবহার করে বিভিন্ন মোবাইল নম্বর ও সোশ্যাল মিডিয়া প্রোফাইল (যেমন : হোয়াটসঅ্যাপ/ফেসবুক/টুইটার/ইত্যাদি) থেকে অধস্তন কর্মকর্তাদের ফোন বা মেসেজ প্রদান করছে। প্রতারক চক্রটি ডিজিটাল প্রযুক্তির অপব্যবহার করে ওটিপি (OTP), পিন নম্বর বা ব্যক্তিগত তথ্য সংগ্রহ করে আর্থিক ক্ষতি সাধনের অপচেষ্টা চালাচ্ছে। মহাপরিচালক, খাদ্য অধিদপ্তর বা খাদ্য মন্ত্রণালয়/খাদ্য অধিদপ্তর/মাঠপর্যায়ের কর্মকর্তাগণের নাম/ছবি ব্যাবহারের মাধ্যমে করা এই ধরনের প্রতারণার শিকার হওয়া থেকে সুরক্ষা পেতে নিম্নোক্ত নির্দেশনাসমূহ কঠোরভাবে মেনে চলার জন্য খাদ্য অধিদপ্তর ও মাঠ পর্যায়ের দপ্তর/কার্যালয়-কে অনুরোধ করা হলো :

১। ফোন কল সংক্রান্ত নির্দেশনা :

- কোনো ব্যক্তি নিজেকে উর্ধ্বতন কর্মকর্তা পরিচয় দিলেও তার নিকট ফোন বা মেসেজে OTP, PIN, Password প্রদান করা যাবে না;
- অপরিচিত বা সন্দেহজনক নম্বর থেকে কল পেলে তাৎক্ষণিকভাবে বিশ্বাস না করে প্রয়োজন হলে অফিসিয়াল নম্বরে যোগাযোগ করে বিষয়টি যাচাই করতে হবে;
- “জরুরি”, “অত্যন্ত গোপনীয়” ইত্যাদি বলে তড়িঘড়ি সিদ্ধান্ত নিতে চাপ দেওয়া প্রতারণার একটি সাধারণ কৌশল এ বিষয়ে সতর্ক থাকতে হবে।

২। ইমেইল ব্যবহার/লিংক ক্লিকে সতর্কতা :

- অপরিচিত বা সন্দেহজনক ইমেইল থেকে প্রেরিত কোনো লিংকে ক্লিক করা বা সংযুক্ত ফাইল (attachment) ডাউনলোড করা থেকে বিরত থাকুন;
- প্রেরকের ইমেইল ঠিকানা (Domain) ভালোভাবে যাচাই না করে কোনো তথ্য আদান-প্রদান করবেন না, অফিসিয়াল যোগাযোগের ক্ষেত্রে শুধুমাত্র অনুমোদিত সরকারি ইমেইল ডোমেইন (dgfood.gov.bd) ব্যবহার নিশ্চিত করতে হবে;
- WhatsApp, messenger বা মোবাইলে মেসেজে কোন বন্ধু, কলিগ বা আত্মীয় স্বজনের নিকট হতে কোন ধরনের পুরস্কার বিজয় বা প্রমোশনাল এড কেউ শেয়ার করলে সেই লিংক ক্লিক করা বা শেয়ার করা থেকে বিরত থাকতে হবে।

৩। সামাজিক যোগাযোগ মাধ্যম (WhatsApp/Messenger ইত্যাদি) :

- উর্ধ্বতন কর্মকর্তার নাম ও ছবি ব্যবহার করে ভুয়া প্রোফাইল তৈরি হতে পারে, নম্বর সেভ না থাকলে শুধুমাত্র ছবি দেখে বিভ্রান্ত হবেন না;
- কোনো মাধ্যমে টাকা, OTP বা ব্যক্তিগত তথ্য চাওয়া হলে তা সরাসরি প্রদান না করে অন্য কোনো নির্ভরযোগ্য মাধ্যমে যাচাই করতে হবে;
- “Do you want to add another device” এ ধরনের মেসেজ আসলে YES/Link ট্যাপ/ক্লিক করা যাবে না;
- WhatsApp কোন কোন ডিভাইসে লিংক করা আছে তা নিয়মিত চেক করতে হবে এবং অপরিচিত ডিভাইসে লিংক করা থাকলে তা অতি দ্রুত ডিসকানেক্ট করতে হবে;
- অপরিচিত লিংক, ফাইল বা অ্যাপ ইনস্টল করা থেকে বিরত থাকতে হবে;

- অপরিচিত নম্বর থেকে আসা ভিডিও কল রিসিভ করা থেকে বিরত থাকতে হবে।

৪। OTP ও পাসওয়ার্ড নিরাপত্তা :

- OTP, PIN, Password, CVV ইত্যাদি অত্যন্ত গোপনীয় তথ্য - এগুলো কখনো কারো সাথে শেয়ার করা যাবে না;
- শক্তিশালী পাসওয়ার্ড ব্যবহার করতে হবে এবং তা নিয়মিত পরিবর্তন করতে হবে;
- একই পাসওয়ার্ড একাধিক অ্যাকাউন্টে ব্যবহার করা থেকে বিরত থাকতে হবে;
- সম্ভব হলে সকল গুরুত্বপূর্ণ অ্যাকাউন্টে Two-Factor Authentication (2FA) চালু রাখতে পারেন।

৫। মোবাইল ও ডিভাইস নিরাপত্তা :

- প্রয়োজনে শুধুমাত্র বিশ্বস্ত উৎস (Google Play Store/App Store) থেকে অ্যাপ ইনস্টল করতে হবে;
- মোবাইল ডিভাইসে Screen Lock (PIN/Password/Fingerprint) ব্যবহার নিশ্চিত করতে হবে;
- অজানা বা সন্দেহজনক কোনো অ্যাপ ইনস্টল করা থেকে বিরত থাকতে হবে;
- মোবাইলে ইনস্টল করা সকল অ্যাপসের পারমিশন চেক করে অপ্রয়োজনীয় পারমিশন রিমুভ করতে হবে।

৬। ব্যাংক ও মোবাইল ফাইন্যান্সিয়াল সার্ভিস (MFS) :

- ব্যাংক বা মোবাইল ফাইন্যান্সিয়াল সার্ভিস (MFS) যেমন- বিকাশ, নগদ বা রকেটের লেনদেন সংক্রান্ত SMS বা OTP প্রাপ্তির ক্ষেত্রে সচেতন থাকুন;
- কোনো সন্দেহজনক লেনদেন পরিলক্ষিত হলে তাৎক্ষণিকভাবে সংশ্লিষ্ট ব্যাংক বা MFS সেবা প্রদানকারীর সাথে যোগাযোগ করুন।

৭। বিভিন্ন ওয়েবসাইটে লগইন :

- ব্যাটিং, চ্যাটিং, ডেটিং, গেমিং, অনলাইন জুয়া ও অন্যান্য সাইটে ভিজিট/ রেজিস্ট্রেশন করা থেকে বিরত থাকতে হবে;
- অফিসিয়াল ইমেইল এড্রেস ব্যবহার করে কোন শপিং সাইট/রেজিস্ট্রেশন করা থেকে বিরত থাকতে হবে।

৮। জরুরি করণীয় :

- প্রতারণার শিকার হলে বিলম্ব না করে সংশ্লিষ্ট উর্ধ্বতন কর্তৃপক্ষ এবং প্রয়োজনে আইন-শৃঙ্খলা রক্ষাকারী বাহিনীকে অবহিত করতে হবে;
- সাইবার নিরাপত্তা সম্পর্কিত যে কোন অভিযোগের জন্য অফিসিয়াল WhatsApp নম্বর - 01308332592 জাতীয় সাইবার সুরক্ষা এজেন্সির হেল্পলাইন নম্বর- 333(8)।

উপরোক্ত দিক-নির্দেশনা যথাযথ অনুসরণের জন্য খাদ্য অধিদপ্তর ও মাঠ পর্যায়ের দপ্তর/কার্যালয়-কে নির্দেশক্রমে অনুরোধ করা হলো। পাশাপাশি ইতোপূর্বে অত্র দপ্তরের পত্রে সাইবার সিকিউরিটি বিষয়ে সচেতনতামূলক অনলাইন প্রশিক্ষণ আয়োজনের জন্য অনুরোধ করা হয় তা বাস্তবায়নের জন্য সংশ্লিষ্ট সকলকে নির্দেশক্রমে অনুরোধ করা হলো। উল্লেখ্য যে, উক্ত প্রশিক্ষণে কম্পিউটার নেটওয়ার্ক ইউনিট, খাদ্য অধিদপ্তরের কর্মকর্তাগণ প্রশিক্ষক হিসেবে সহায়তা প্রদান করবেন।

২৫-০৩-২০২৬
মোঃ আনিসুর রহমান
প্রোগ্রামার

বিতরণ (জ্যেষ্ঠতার ক্রমানুসারে নয়):

১। অতিরিক্ত মহাপরিচালক (চলতি দায়িত্ব), অতিরিক্ত মহাপরিচালকের দপ্তর, খাদ্য অধিদপ্তর।
২। পরিচালক (বিকল্প কর্মকর্তা), প্রশাসন বিভাগ, খাদ্য অধিদপ্তর।
৩। পরিচালক, হিসাব ও অর্থ বিভাগ, খাদ্য অধিদপ্তর।
৪। পরিচালক, সংগ্রহ বিভাগ, খাদ্য অধিদপ্তর।
৫। পরিচালক, সরবরাহ, বন্টন ও বিপণন বিভাগ, খাদ্য অধিদপ্তর।

৬। পরিচালক, প্রশিক্ষণ বিভাগ, খাদ্য অধিদপ্তর।
৭। পরিচালক (চলতি দায়িত্ব), চলাচল, সংরক্ষণ ও সাইলো বিভাগ, খাদ্য অধিদপ্তর।
৮। পরিচালক (চলতি দায়িত্ব), পরিদর্শন, উন্নয়ন ও কারিগরি সেবা বিভাগ, খাদ্য অধিদপ্তর।
৯। প্রধান মিলার, প্রধান মিলার এর দপ্তর, পোস্তগোলা সরকারি আধুনিক ময়দা মিল, ঢাকা।
১০। সিস্টেম এনালিস্ট, কম্পিউটার নেটওয়ার্ক ইউনিট, খাদ্য অধিদপ্তর।
১১। তত্ত্বাবধায়ক প্রকৌশলী (অতিরিক্ত দায়িত্ব), নির্মাণ ও রক্ষণাবেক্ষণ ইউনিট, খাদ্য অধিদপ্তর।
১২। আঞ্চলিক খাদ্য নিয়ন্ত্রক (সকল)।
১৩। সাইলো অধীক্ষক (সকল)।
১৪। প্রধান নিয়ন্ত্রক, ঢাকা রেশনিং, ঢাকা।
১৫। অতিরিক্ত পরিচালক, অভ্যন্তরীণ নিরীক্ষা বিভাগ, খাদ্য অধিদপ্তর এবং
১৬। অতিরিক্ত পরিচালক (চলতি দায়িত্ব), এমআইএসএন্ডএম বিভাগ, খাদ্য অধিদপ্তর।

স্মারক নম্বর: ১৩.০১.০০০০.০০০.১০০.৩১.০০২৩.২১.৭৪/১ (১)

তারিখ: ১১ চৈত্র ১৪৩২ বঙ্গাব্দ
২৫ মার্চ ২০২৬ খ্রিস্টাব্দ

সদয় জ্ঞাতার্থে/জ্ঞাতার্থে (জ্যেষ্ঠতার ক্রমানুসারে নয়):

মহাপরিচালকের একান্ত সচিব, মহাপরিচালকের দপ্তর, খাদ্য অধিদপ্তর।

২৫-০৩-২০২৬
মোঃ আনিসুর রহমান
প্রোগ্রামার