নাম: _____ তারিখ: _____ নম্বর: _____

অনলাইন প্রতারণা ও সোশ্যাল ইঞ্জিনিয়ারিং সুরক্ষা গাইড

ইমেল ফিশিং, স্পুফ করা ডোমেইন, ভিশিং, সাপোর্ট স্ক্যাম, আউট-অফ-ব্যান্ড যাচাই, BEC

অনলাইন প্রতারণা শিক্ষণ পরিচিতি

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে অনলাইন স্ক্যাম প্রতিরক্ষা বিষয়ে গাইড করবে। আপনি ভুয়া ফিশিং ওয়েবসাইট, সোশ্যাল ইঞ্জিনিয়ারিং কৌশল, সাপোর্ট স্ক্যাম, ওয়্যার ফ্রডের পথ এবং পেমেন্ট যাচাই পদ্ধতি সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/online-scam/

আপনার অনলাইন স্ক্যাম সুরক্ষা শেখার রোডম্যাপ

- সাপোর্ট স্ক্যাম ও টাইপোস্কোয়াটিং ডোমেইনের সাধারণ নির্দেশক শনাক্ত করুন।
- স্পুফিংয়ের বিরুদ্ধে ইমেইল যাচাই প্রোটোকল (SPF, DKIM, DMARC) বাস্তবায়ন করুন।
- ব্যবসায়িক ওয়্যার প্রতারণা রোধে আউট-অফ-ব্যান্ড লেনদেন যাচাই প্রতিষ্ঠা করুন।

অনলাইন প্রতারণা গাইড নির্দেশনা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। অনলাইন প্রতারণা থেকে সুরক্ষা বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

অনলাইন প্রতারণা ও সোশ্যাল ইঞ্জিনিয়ারিং থেকে সুরক্ষা (ভূমিকা)

অনলাইন প্রতারণা ফিশিং, সাপোর্ট পপ-আপ, ভিশিং ও ওয়্যার ফ্রডের মাধ্যমে মানুষের আচরণকে কাজে লাগায়। আউট-অব-ব্যান্ড লেনদেন যাচাই এবং SPF/DKIM/DMARC ডোমেইন নিয়ম কার্যকর করলে গেটওয়েতেই সোশ্যাল ইঞ্জিনিয়ারিংয়ের পথ ঠেকাতে সাহায্য করে।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1. সাপোর্ট স্ক্যামের প্রধান লক্ষণ কী?
   - A. আপনার সিস্টেম সংক্রমিত বলে দাবি করে একটি ফোন নম্বরে কল করতে বলা পপ-আপ
   - B. অফিসিয়াল রেজিস্ট্রি থেকে ডাউনলোড করা স্বয়ংক্রিয় নিরাপত্তা আপডেট
   - C. কর্পোরেট ডোমেইনে ক্রেডেনশিয়াল পূরণ করতে অস্বীকার করা একটি পাসওয়ার্ড ম্যানেজার
   - D. বাহ্যিক ড্রাইভ কনফিগারেশনে চলমান ব্যাকগ্রাউন্ড ফাইল ব্যাকআপ

2. ব্যাংকের তথ্য চুরির জন্য কোন কৌশল জাল প্রেরকের ডোমেইন ব্যবহার করে?
   - A. ইমেইল ফিশিং
   - B. পোর্ট স্ক্যানিং
   - C. মেমরি ইনজেকশন
   - D. ক্রিপ্টোগ্রাফিক শ্রেডিং

3. ওয়্যার ট্রান্সফার জালিয়াতি কী বোঝায়?
   - A. সোশ্যাল ইঞ্জিনিয়ারিং ব্যবহার করে ভুক্তভোগীদের ভুয়া কর্পোরেট অ্যাকাউন্টে অর্থ পাঠাতে প্রতারিত করা
   - B. র‍্যানসমওয়্যার পেলোড ব্যবহার করে সিস্টেম ডেটাবেস এনক্রিপ্ট করা
   - C. SQL ইনজেকশন কমান্ডের মাধ্যমে ডাটাবেস কোয়েরি করা
   - D. অফলাইন স্টোরেজ ডিস্কে সিস্টেম ফাইলের ব্যাকআপ রাখা

4. প্রতারকেরা কেন ভুয়া কেনাকাটার ওয়েবসাইট তৈরি করে?
   - A. ক্রেতাদের ক্রেডিট কার্ডের তথ্য ও পেমেন্ট ক্রেডেনশিয়াল চুরি করতে
   - B. স্যান্ডবক্স করা ম্যালওয়্যার বিশ্লেষণের ডেটাবেস টেবিল হোস্ট করতে
   - C. অনলাইন অর্ডার পৌঁছানো দ্রুত করতে
   - D. বিনামূল্যে নতুন ওয়েবসাইট ডিজাইন পরীক্ষা করতে

5. ভিশিং বলতে কী বোঝায়?
   - A. পরিচয় ও ক্রেডেনশিয়াল চুরির জন্য ফোন নেটওয়ার্কে ভয়েস ফিশিং প্রতারণা
   - B. অনিরাপদ সিস্টেম ডিভাইসের জন্য স্থানীয় নেটওয়ার্ক স্ক্যান করা
   - C. অননুমোদিত লঙ্ঘনের পর সিস্টেম ডাটাবেস পুনরুদ্ধার করা
   - D. নিরাপদ ভার্চুয়াল কনটেইনারের ভেতরে অবিশ্বস্ত কোড চালানো

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. ফিশিং প্রতারণা শুধু সাধারণ ব্যবহারকারীদের লক্ষ্য করে, কখনও নির্বাহীদের হোয়েলিং লক্ষ্যবস্তুদের নয়।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. স্পুফ করা ডোমেইন প্রায়ই ছোট টাইপো (যেমন amaz0n.com) ব্যবহার করে বিশ্বস্ত ব্র্যান্ডের অনুকরণ করে।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. কলারকে রিমোট অ্যাক্সেস দিয়ে সাপোর্ট প্রতারণা সমাধান করা যায়।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. সোশ্যাল ইঞ্জিনিয়ারিং নিরাপত্তা নিয়ম এড়াতে ভয় ও তাড়াহুড়োর মতো মানুষের মনস্তত্ত্বকে কাজে লাগায়।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. ওয়্যার ট্রান্সফারের অনুরোধ সবসময় আউট-অব-ব্যান্ড যোগাযোগ চ্যানেলের মাধ্যমে যাচাই করা উচিত।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. ব্যবহারকারীকে ঠকানো প্রতারণামূলক ইমেইলকে বলা হয় _____ ।
2. বিশ্বস্ত ব্র্যান্ডের অনুকরণে তৈরি ওয়েব ঠিকানাকে বলা হয় _____ ।
3. ব্যাংকের তথ্য লক্ষ্য করা ভয়েস প্রতারণাকে বলা হয় _____ ।
4. ভাইরাস অপসারণের জন্য অর্থ চাওয়া পপ-আপ হলো একটি সাপোর্ট _____ ।
5. পেমেন্ট অনুরোধ নিশ্চিত করতে আউট-অফ-ব্যান্ড _____ দরকার।
6. ব্যবসায়িক লেনদেন চোরের অ্যাকাউন্টে ঘুরিয়ে দেওয়া হলো _____ ।

পরিভাষা শব্দভাণ্ডার

ইমেইল ওয়্যার জালিয়াতি ফিশিং ভিশিং ম্যালওয়্যার যাচাইকরণ স্ক্যাম স্পুফড

এখানে আপনার উত্তর লিখুন:

1.
2.
3.
4.
5.
6.

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

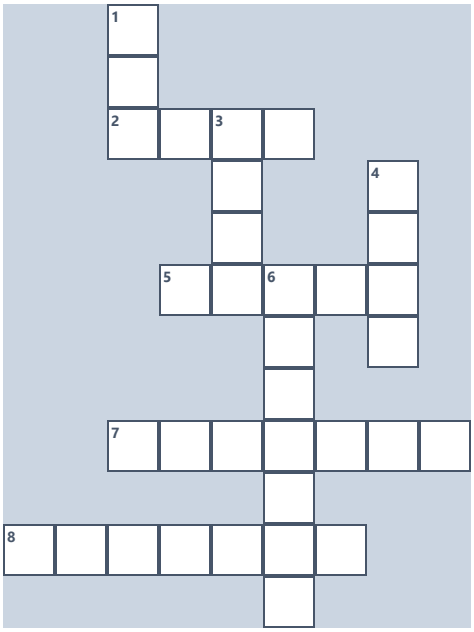
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

☐	**1. ফিশিং**	**A**	ব্যাংক লেনদেন প্রতারণার মাধ্যমে অপরাধীদের অ্যাকাউন্টে সরিয়ে নেওয়া।
☐	**2. স্পুফড**	**B**	ভুক্তভোগীদের কাছ থেকে অর্থ বা লগইন তথ্য চুরির উদ্দেশ্যে তৈরি প্রতারণামূলক পরিকল্পনা।
☐	**3. ভিশিং**	**C**	মোবাইল অ্যাকাউন্টের ক্রেডেনশিয়াল চুরি করতে প্রতারণামূলক টেক্সট মেসেজ পাঠানো।
☐	**4. প্রতারণা**	**D**	ক্রেডেনশিয়াল ও অ্যাকাউন্টের তথ্য চুরির উদ্দেশ্যে তৈরি প্রতারণামূলক ভয়েস কল।
☐	**5. যাচাইকরণ**	**E**	সি-লেভেল নির্বাহীদের ক্রেডেনশিয়াল চুরির লক্ষ্যে চালানো লক্ষ্যভিত্তিক ফিশিং আক্রমণ।
☐	**6. ওয়্যার ট্রান্সফার**	**F**	বৈধ মনে হওয়ার জন্য নকল করা ইমেইল প্রেরক বা ওয়েবসাইট ঠিকানা।
☐	**7. হোয়েলিং**	**G**	লগইন তথ্য ও পাসওয়ার্ড চুরির উদ্দেশ্যে তৈরি প্রতারণামূলক ইমেইল প্রচারণা।
☐	**8. স্মিশিং**	**H**	একটি বিশ্বস্ত বিকল্প যোগাযোগ পদ্ধতিতে পেমেন্টের বিবরণ নিশ্চিত করা।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

2. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4)

5. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5)

7. পরিচয়-তথ্য ও অ্যাকাউন্টের বিবরণ চুরির প্রতারণামূলক ফোনকল (7)

8. মোবাইল অ্যাকাউন্টের লগইন তথ্য চুরির জন্য প্রতারণামূলক টেক্সট বার্তা পাঠানো (7)

উপর-নিচ

1. আসল জিনিসের অবিকল অনুকরণ (3)

3. ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি (4)

4. ভুক্তভোগীর কাছ থেকে অর্থ বা লগইন সুবিধা হাতানোর প্রতারণামূলক ছক (4)

6. ব্যাংক লেনদেন অপরাধীর অ্যাকাউন্টে ঘুরিয়ে দেওয়ার প্রতারণা (7)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

2 পাশাপাশি: নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর):

5 পাশাপাশি: ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর):

7 পাশাপাশি: পরিচয়-তথ্য ও অ্যাকাউন্টের বিবরণ চুরির প্রতারণামূলক ফোনকল (7 অক্ষর):

8 পাশাপাশি: মোবাইল অ্যাকাউন্টের লগইন তথ্য চুরির জন্য প্রতারণামূলক টেক্সট বার্তা পাঠানো (7 অক্ষর):

উপর-নিচ

1 উপর-নিচ: আসল জিনিসের অবিকল অনুকরণ (3 অক্ষর):

3 উপর-নিচ: ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি (4 অক্ষর):

4 উপর-নিচ: ভুক্তভোগীর কাছ থেকে অর্থ বা লগইন সুবিধা হাতানোর প্রতারণামূলক ছক (4 অক্ষর):

6 উপর-নিচ: ব্যাংক লেনদেন অপরাধীর অ্যাকাউন্টে ঘুরিয়ে দেওয়ার প্রতারণা (7 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

ব দি শ জা রা দে ট ই মে র ক সি দ ঠ হ
সা শ মে দে রা কি ঋ মে ম্যা তে না নে ছ য প
উ অ উ ঋ মা বা য ই ফ ল বা ম দে তি ভ
ঘ রে ল ষ ফ ঘ দ ল হ স ও ভ রি মি ঢ
ষ ষ ক রি সি ভ না তি তা ড ঊ য়্যা নি প্র রা
তি কি ন থ সে য়ে ঊ ও লি গ নি জা র তা পি
য়া ঋ জি লি ট স ভ ণ য়্যা জে গ স ঘ র রে
লি দি মি ঋ পা জা উ অ জে র কা গ ম ণা আ
জা ঘ কি ঘ ঝ লি ণ ধ গ সি জা রি শ ছ দ
ট সে জি নি ঝ য়া রে পে জ আ আ লি রে মা স
ক্স মে তি দে রি তি ফ সি তি সে খ স য়া বে উ
টে ট সে দি দা ল প আ সি জে বি বি য তি ড
দ ষ সা ফ ল ল গ তা কে ণ রা রি ণ জে ই
কে পে ঠ পি ঊ বে সে ই বে উ ণ ল জে ঢ ফ
কি মে কা দা ঋ ল জে বে ন ঠ বি কে লে পা ম

পরিভাষা শব্দতালিকা

ভয়েসজালিয়াতি | প্রতারণা | ওয়্যারজালিয়াতি | টেক্সটজালিয়াতি | ম্যালওয়্যার | ইমেইল | লগইন | নকল

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. ভয়েসজালিয়াতি

B. প্রতারণা

C. ওয়্যারজালিয়াতি

D. টেক্সটজালিয়াতি

E. ম্যালওয়্যার

F. ইমেইল

G. লগইন

H. নকল

সংজ্ঞা ও মিলের ঘর

1. ভুক্তভোগীর কাছ থেকে অর্থ বা লগইন সুবিধা হাতানোর প্রতারণামূলক ছক।

2. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার।

3. ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি।

4. আসল জিনিসের অবিকল অনুকরণ।

5. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া।

6. ব্যাংক লেনদেন অপরাধীর অ্যাকাউন্টে ঘুরিয়ে দেওয়ার প্রতারণা।

7. পরিচয়-তথ্য ও অ্যাকাউন্টের বিবরণ চুরির প্রতারণামূলক ফোনকল।

8. মোবাইল অ্যাকাউন্টের লগইন তথ্য চুরির জন্য প্রতারণামূলক টেক্সট বার্তা পাঠানো।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. জা য়া ভ লি তি স য়ে
2. ও র তি য়া লি জা য়্যা
3. ও ম্যা র য়্যা ল
4. ন ই ল গ
5. ণা প্র র তা
6. য়া ট লি টে জা তি ক্স
7. ই ই ল মে
8. ল ক ন

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	যেসব ডিভাইস হ্যাক হতে পারে			
2	প্রতারকরা প্রায়ই যেসব বাক্যাংশ ব্যবহার করে			
3	প্রতারকরা যেসব পেমেন্ট পদ্ধতি চায়			
4	অনলাইন প্রতারণার ধরন			
5	সত্যি হওয়ার পক্ষে অতিরিক্ত ভালো অফার			
6	প্রতারণার রিপোর্ট করার জায়গা			
7	সাইবার নিরাপত্তার সঙ্গে সম্পর্কিত শব্দ			
8	প্রতারণা সম্পর্কে আপনি যাদের সতর্ক করতে পারেন			
9	যা যা আপনি ব্যাকআপ করেন			
10	ইমেইলে সতর্কতার লক্ষণ			
11	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
12	একটি অনলাইন শপ যাচাই করার উপায়			
13	আপনার অ্যাকাউন্ট সুরক্ষিত রাখার উপায়			
14	প্রতারণার শিকার হলে যা করবেন			
15	ডেটা ফাঁসের পর যা করবেন			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: কর্পোরেট ওয়্যার ট্রান্সফার প্রতারণা প্রতিরোধ



পরিস্থিতি: একটি অর্থ বিভাগ একটি স্পুফ করা ভেন্ডর অ্যাড্রেস থেকে জরুরি ইমেইল পায়, যাতে অনুরোধ করা হয় ভবিষ্যতের ইনভয়েসের ওয়্যার একটি নতুন রাউটিং নম্বরে পাঠানো হোক।

আলোচনার প্রশ্ন: ওয়্যার প্রতারণা যাচাই নীতির রূপরেখা দিন এবং ইমেইল প্রমাণীকরণ ব্লক উল্লেখ করুন।

কেস স্টাডি 2: নির্বাহীকে লক্ষ্য করা হোয়েলিং ফিশিং ঘটনা



পরিস্থিতি: একজন নির্বাহী একটি নিরাপদ বোর্ড-সভার নথি আছে দাবি করা ফিশিং লিংকে ক্লিক করে একটি স্পুফ করা পোর্টালে তাঁর প্রধান কর্পোরেট ক্রেডেনশিয়াল দিয়ে দেন।

আলোচনার প্রশ্ন: ঘটনা-সাড়া প্রদানের ধাপগুলো বিস্তারিত বর্ণনা করুন এবং নির্বাহীদের লগইন কীভাবে অডিট করবেন তা ব্যাখ্যা করুন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12

খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24

ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36

য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48

ূ=49 ৃ=50 ে=51 ৈ=52 ো=53 ৌ=54 ং=55 ঃ=56 ঁ=57 ্=58 ়=59

37	45	17	45	3	12	38	26		29	46	37	59	51		33	46	40	46	55

32	58	38	17	45	38	26	45		30	38	48	31

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: অনলাইন প্রতারণা কী?

একটি প্রতারণামূলক পরিকল্পনা, যেখানে ডিজিটাল মাধ্যম ব্যবহার করে ভুক্তভোগীদের অর্থ পাঠাতে বা ব্যক্তিগত ক্রেডেনশিয়াল দিতে প্রতারিত করা হয়।

Q2: ইমেইল ফিশিংয়ের প্রধান সূচক কী?

জরুরি অবস্থার (যেমন অ্যাকাউন্ট স্থগিত) দাবি করে এবং সরকারি ডোমেইনের সঙ্গে না মেলা লিংকে যেতে বলা বার্তা।

Q3: টাইপোস্কোয়াটিং কী?

ভুয়া ফিশিং সাইট চালাতে জনপ্রিয় ব্র্যান্ডের সাধারণ বানান-ভুলসহ ডোমেইন (যেমন amaz0n.com) নিবন্ধন করা।

Q4: সাপোর্ট স্ক্যাম কী?

একটি পপ-আপ, যা দাবি করে আপনার পিসি সংক্রমিত এবং একটি নম্বরে কল করে ভুয়া ক্লিনআপ সফটওয়্যার বা রিমোট অ্যাক্সেস সেবার জন্য অর্থ দিতে বলে। [1]

Q5: ভিশিং কী?

ভিকটিমদের ব্যাংক অ্যাকাউন্ট বা লগইনের তথ্য দিতে ভোলাতে ভয়েস ফোন কল ব্যবহার করা ফিশিং আক্রমণ।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: ওয়্যার ফ্রড বলতে কী বোঝায়?

বিক্রেতা বা নির্বাহী সেজে পেমেন্ট লেনদেন প্রতারণামূলক অ্যাকাউন্টে সরিয়ে নেওয়া।

Q7: হোয়েলিং কী?

স্পিয়ার ফিশিংয়ের একটি অত্যন্ত লক্ষ্যভিত্তিক রূপ, যা সরাসরি C-লেভেল কর্পোরেট নির্বাহীদের মতো উচ্চমূল্যের লক্ষ্যকে নিশানা করে।

Q8: স্মিশিং কী?

মোবাইল ডিভাইসে পাঠানো প্রতারণামূলক টেক্সট বার্তা, যাতে ভুয়া পোর্টাল বা ট্র্যাকিং হালনাগাদের লিংক থাকে।

Q9: আউট-অব-ব্যান্ড যাচাই কেন গুরুত্বপূর্ণ?

এটি আলাদা যোগাযোগ মাধ্যম (যেমন ফোন কল) ব্যবহার করে লেনদেনের বিবরণ নিশ্চিত করে, ফলে আপসকৃত ইমেইল থ্রেড এড়ানো যায়।

Q10: ভুয়া এসক্রো প্রতারণা কীভাবে কাজ করে?

প্রতারকরা ভুয়া এসক্রো সাইট তৈরি করে, দাবি করে অর্থ নিরাপদে রাখা আছে, তারপর ক্রেতার ওয়্যার ট্রান্সফার করা অর্থ চুরি করে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: প্রতারকরা ওয়্যার ফ্রড চালাতে কীভাবে BEC (Business Email Compromise) ব্যবহার করে?

এরা একজন বৈধ কর্মীর ইমেইল অ্যাকাউন্ট হাইজ্যাক করে, ইনভয়েসের থ্রেড পর্যবেক্ষণ করে এবং প্রতারণামূলক ব্যাংক অ্যাকাউন্টসহ হালনাগাদ বিলিং তথ্য পাঠায়।

Q2: অনলাইন প্রতারণায় IDN হোমোগ্রাফ আক্রমণের ঝুঁকি কী?

আসল ব্র্যান্ডের নকল করা ভুয়া ডোমেইন নিবন্ধন করতে সাধারণ অক্ষরের মতো হুবহু দেখতে non-ASCII অক্ষর (যেমন Cyrillic 'a') ব্যবহার করা।

Q3: প্রতারণা শনাক্তকরণে ইমেইল হেডার পরীক্ষা কেন গুরুত্বপূর্ণ?

এটি প্রকৃত উৎস সার্ভার IP এবং SPF/DKIM যাচাইয়ের অবস্থা প্রকাশ করে, যা দেখায় প্রেরকের ডোমেইন জাল কিনা।

Q4: সাপোর্ট স্ক্যামাররা কীভাবে রিমোট ডেস্কটপ সফটওয়্যারের অপব্যবহার করে?

এরা AnyDesk বা TeamViewer-এর মতো ইউটিলিটি ব্যবহার করে ভুক্তভোগীর ডিভাইসে সংযোগ করে, ম্যালওয়্যার বসায় এবং সংরক্ষিত পাসওয়ার্ড চুরি করে।

Q5: অ্যাডভান্স-ফি স্ক্যামের লক্ষ্য কী?

অস্তিত্বহীন বড় আর্থিক পুরস্কারের বিনিময়ে ভুক্তভোগীদের অগ্রিম প্রক্রিয়াকরণ ফি দিতে প্রতারিত করা।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: স্ক্যামাররা লক্ষ্যভিত্তিক ফিশিংয়ে কীভাবে সোশ্যাল মিডিয়া প্রোফাইলিং ব্যবহার করে?

বিশ্বাসযোগ্য স্পিয়ার-ফিশিং ইমেইল লিখতে এরা কর্পোরেট সাংগঠনিক কাঠামো ও কর্মীদের নাম সংকলন করে।

Q7: ভুয়া ওয়েব শপ কেন বড় ছাড় দেয়?

ক্রেতাদের প্রলুব্ধ করে ক্রেডিট কার্ডের তথ্য দিতে বাধ্য করতে এবং কার্ডিং ফোরামে পুনরায় ব্যবহার বা বিক্রির জন্য ক্রেডেনশিয়াল হাতিয়ে নিতে।

Q8: DMARC রেকর্ড কীভাবে ফিশিং প্রতারণা ব্লক করে?

DMARC ডোমেইন মালিকদের অনুরোধ করতে দেয় যেন প্রাপকরা সারিবদ্ধ SPF ও DKIM যাচাইয়ে ব্যর্থ মেইল কোয়ারেন্টাইন বা প্রত্যাখ্যান করে, যা সরাসরি স্পুফিং আটকায়। [5]

Q9: ক্রেডেনশিয়াল হার্ভেস্টিং পোর্টালের হুমকি কী?

Microsoft 365 বা Google workspace-এর হুবহু অনুকরণে তৈরি স্পুফ করা ল্যান্ডিং পেজ, যা লগইন ক্রেডেনশিয়াল দেওয়া মাত্রই চুরি করে।

Q10: নিরাপত্তা টিম কীভাবে প্রতারণামূলক ডোমেইন রিপোর্ট ও নিষ্ক্রিয় করে?

রেজিস্ট্রারের অ্যাবিউজ ইমেইল, হোস্টিং প্রদানকারী ও Google Safe Browsing রেজিস্ট্রিতে প্রতারণার প্রমাণ জমা দিয়ে।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

2025 সালে FBI-র IC3-তে সবচেয়ে বেশি রিপোর্ট হওয়া অপরাধের ধরন ছিল ফিশিং ও স্পুফিং, যেখানে অভিযোগ এসেছিল 191,561টি। [2]

2. নিরাপত্তা ইনসাইট

Business Email Compromise (BEC) 2025 সালে FBI-এর IC3-তে জানানো $3 বিলিয়নের বেশি ক্ষতির কারণ হয়েছে। [2]

3. নিরাপত্তা ইনসাইট

টাইপো-স্কোয়াট করা ডোমেইন আসল ব্র্যান্ডের নাম থেকে এক-দুটি অক্ষরে আলাদা হয়, তাই এক পলক দেখে ধরা নাও পড়তে পারে।

4. নিরাপত্তা ইনসাইট

2025 সালে FBI-এর IC3-তে জানানো টেক সাপোর্ট প্রতারণায় ক্ষতির পরিমাণ ছিল 2.1 বিলিয়ন ডলারের বেশি। [2]

5. নিরাপত্তা ইনসাইট

ব্রাউজার পিউনিকোড কনফিগারেশন না দেখালে ব্রাউজারের ঠিকানা বারে হোমোগ্রাফ আক্রমণ হুবহু একই রকম দেখায়।

6. নিরাপত্তা ইনসাইট

SMS টেক্সট প্রতারণা (স্মিশিং) লিংকসহ সংক্ষিপ্ত, জরুরি বার্তা ব্যবহার করে, ফলে ভুক্তভোগীরা প্রতারণা ধরার মতো প্রসঙ্গ কম পায়।

7. সিকিউরিটি ইনসাইট

হোয়েলিং আক্রমণ নির্বাহীদের ইমেইলকে লক্ষ্য করে, কারণ তাঁরা বড় অঙ্কের ওয়্যার ট্রান্সফার পেমেন্টের অ্যাক্সেস নিয়ন্ত্রণ করেন।

8. সিকিউরিটি ইনসাইট

পরিচিত, সংরক্ষিত ফোন নম্বরে কল করে পেমেন্ট পরিবর্তন যাচাই করা BEC ওয়্যার জালিয়াতির বিরুদ্ধে একটি মূল প্রতিরক্ষা।

9. সিকিউরিটি ইনসাইট

ভুয়া এসক্রো ওয়েবসাইট অনলাইন মার্কেটপ্লেসের একটি প্রচলিত প্রতারণা: এগুলো নিরাপদ পেমেন্ট সেবার মতো দেখায় কিন্তু ক্রেতার ওয়্যার ট্রান্সফার চুরি করে।

10. নিরাপত্তা ইনসাইট

Google Safe Browsing ফিশিং বা ম্যালওয়্যারের জন্য চিহ্নিত সাইট খোলার আগে ব্যবহারকারীদের সতর্ক করে।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[1] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 — সঠিক উত্তর: A

শিক্ষণ নোট

সাপোর্ট স্ক্যামের প্রধান লক্ষণ কী? → আপনার সিস্টেম সংক্রমিত বলে দাবি করে একটি ফোন নম্বরে কল করতে বলা পপ-আপ

2 প্রশ্ন 2 — সঠিক উত্তর: A

শিক্ষণ নোট

ব্যাংকের তথ্য চুরির জন্য কোন কৌশল জাল প্রেরকের ডোমেইন ব্যবহার করে? → ইমেইল ফিশিং

3 প্রশ্ন 3 — সঠিক উত্তর: A

শিক্ষণ নোট

ওয়্যার ট্রান্সফার জালিয়াতি কী বোঝায়? → সোশ্যাল ইঞ্জিনিয়ারিং ব্যবহার করে ভুক্তভোগীদের ভুয়া কর্পোরেট অ্যাকাউন্টে অর্থ পাঠাতে প্রতারিত করা

4 প্রশ্ন 4 — সঠিক উত্তর: A

শিক্ষণ নোট

প্রতারকেরা কেন ভুয়া কেনাকাটার ওয়েবসাইট তৈরি করে? → ক্রেতাদের ক্রেডিট কার্ডের তথ্য ও পেমেন্ট ক্রেডেনশিয়াল চুরি করতে

5 প্রশ্ন 5 — সঠিক উত্তর: A

শিক্ষণ নোট

ভিশিং বলতে কী বোঝায়? → পরিচয় ও ক্রেডেনশিয়াল চুরির জন্য ফোন নেটওয়ার্কে ভয়েস ফিশিং প্রতারণা

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: ফিশিং নির্বাহীদেরও লক্ষ্য করে; হোয়েলিং হলো ঊর্ধ্বতন নেতাদের লক্ষ্য করা ফিশিং।

7 প্রশ্ন 7 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

স্পুফ করা ডোমেইন প্রায়ই ছোট টাইপো (যেমন amaz0n.com) ব্যবহার করে বিশ্বস্ত ব্র্যান্ডের অনুকরণ করে।

8 প্রশ্ন 8 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: সাপোর্ট প্রতারককে রিমোট অ্যাক্সেস দিলে সে ম্যালওয়্যার বসাতে ও ডেটা চুরি করতে পারে।

9 প্রশ্ন 9 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সোশ্যাল ইঞ্জিনিয়ারিং নিরাপত্তা নিয়ম এড়াতে ভয় ও তাড়াহুড়োর মতো মানুষের মনস্তত্ত্বকে কাজে লাগায়।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

ওয়্যার ট্রান্সফারের অনুরোধ সবসময় আউট-অব-ব্যান্ড যোগাযোগ চ্যানেলের মাধ্যমে যাচাই করা উচিত।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

G 1. ফিশিং	F 2. স্পুফড	D 3. ভিশিং	B 4. প্রতারণা
H 5. যাচাইকরণ	A 6. ওয়্যার ট্রান্সফার	E 7. হোয়েলিং	C 8. স্মিশিং

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 ফিশিং	2 স্পুফড	3 ভিশিং	4 স্ক্যাম
5 যাচাইকরণ	6 ওয়্যার জালিয়াতি		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 B – প্রতারণা	2 E – ম্যালওয়্যার	3 F – ইমেইল	4 H – নকল
5 G – লগইন	6 C – ওয়্যারজালিয়াতি	7 A – ভয়েসজালিয়াতি	8 D – টেক্সটজালিয়াতি

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা ফিশিং, স্পুফড ও ভিশিং নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ব	দি	শ	জা	রা	দে	ট	ই	মে	র	ক	সি	দ	ঠ	হ
সা	শ	মে	দে	রা	কি	ঋ	মে	ম্যা	তে	না	নে	ছ	য	প
উ	অ	উ	ঋ	মা	বা	য	ই	ফ	ল	বা	ম	দে	তি	ভ
ঘ	রে	ল	ষ	ফ	ঘ	দ	ল	হ	স	ও	ভ	রি	মি	ঢ
ষ	ষ	ক	রি	সি	ভ	না	তি	তা	ড	ঊ	য়্যা	নি	প্র	রা
তি	কি	ন	থ	সে	য়ে	ঊ	ও	লি	গ	নি	জা	র	তা	পি
য়া	ঋ	জি	লি	ট	স	ভ	ণ	য়্যা	জে	গ	স	ঘ	র	রে
লি	দি	মি	ঋ	পা	জা	উ	অ	জে	র	কা	গ	ম	ণা	আ
জা	ঘ	কি	ঘ	ঝ	লি	ণ	ধ	গ	সি	জা	রি	শ	ছ	দ
ট	সে	জি	নি	ঝ	য়া	রে	পে	জ	আ	আ	লি	রে	মা	স
ক্স	মে	তি	দে	রি	তি	ফ	সি	তি	সে	খ	স	য়া	বে	উ
টে	ট	সে	দি	দা	ল	প	আ	সি	জে	বি	বি	য	তি	ড
দ	ষ	সা	ফ	ল	ল	গ	তা	কে	ণ	রা	রি	ণ	জে	ই
কে	পে	ঠ	পি	ঊ	বে	সে	ই	বে	উ	ণ	ল	জে	ঢ	ফ
কি	মে	কা	দা	ঋ	ল	জে	বে	ন	ঠ	বি	কে	লে	পা	ম

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

2 পাশাপাশি: লগইন নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর)

5 পাশাপাশি: ম্যালওয়্যার ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর)

7 পাশাপাশি: ভয়েসজালিয়াতি পরিচয়-তথ্য ও অ্যাকাউন্টের বিবরণ চুরির প্রতারণামূলক ফোনকল (7 অক্ষর)

8 পাশাপাশি: টেক্সটজালিয়াতি মোবাইল অ্যাকাউন্টের লগইন তথ্য চুরির জন্য প্রতারণামূলক টেক্সট বার্তা পাঠানো (7 অক্ষর)

উপর-নিচ

1 উপর-নিচ: নকল আসল জিনিসের অবিকল অনুকরণ (3 অক্ষর)

3 উপর-নিচ: ইমেইল ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি (4 অক্ষর)

4 উপর-নিচ: প্রতারণা ভুক্তভোগীর কাছ থেকে অর্থ বা লগইন সুবিধা হাতানোর প্রতারণামূলক ছক (4 অক্ষর)

6 উপর-নিচ: ওয়্যারজালিয়াতি ব্যাংক লেনদেন অপরাধীর অ্যাকাউন্টে ঘুরিয়ে দেওয়ার প্রতারণা (7 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1.	জায়াভলিতিসয়ে	ভয়েসজালিয়াতি	5.	ণাপ্ররতা	প্রতারণা
2.	ওরতিয়ালিজায়্যা	ওয়্যারজালিয়াতি	6.	য়াটলিটেজাতিক্স	টেক্সটজালিয়াতি
3.	ওম্যারয়্যাল	ম্যালওয়্যার	7.	ইইলমে	ইমেইল
4.	নইলগ	লগইন	8.	লকন	নকল

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"যাচাইকরণ দিয়ে ফিশিং প্রচারণা ধরুন"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: কর্পোরেট ওয়্যার ট্রান্সফার প্রতারণা প্রতিরোধ

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি অর্থ বিভাগ একটি স্পুফ করা বিক্রেতা ঠিকানা থেকে জরুরি ইমেল পায়, যাতে অনুরোধ করা হয়েছে ভবিষ্যৎ ইনভয়েসের ওয়্যার একটি নতুন রাউটিং নম্বরে পাঠাতে।
- প্রস্তাবিত কৌশল ও সমাধান: সব পেমেন্টের জন্য দ্বৈত-অনুমোদন নীতি কার্যকর করুন। আগে থেকে সংরক্ষিত ফোন নম্বর ব্যবহার করে আউট-অফ-ব্যান্ড যাচাই চালু করুন এবং গেটওয়েতে ভুয়া ডোমেইনের ইমেল ব্লক করুন।

B কেস স্টাডি 2: নির্বাহীকে লক্ষ্য করা হোয়েলিং ফিশিং ঘটনা

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একজন নির্বাহী নিরাপদ বোর্ড-মিটিং নথি আছে বলে দাবি করা একটি ফিশিং লিংকে ক্লিক করেন এবং একটি স্পুফ করা পোর্টালে তাঁর প্রধান কর্পোরেট ক্রেডেনশিয়াল দিয়ে দেন।
- প্রস্তাবিত কৌশল ও সমাধান: নির্বাহীর ডিভাইসটি আলাদা করুন। কর্পোরেটের সব সেশন টোকেন ও ক্রেডেনশিয়াল রিসেট করুন। ডেটা বাইরে যাওয়ার চিহ্ন খুঁজতে অ্যাক্সেস লগ পর্যালোচনা করুন এবং সব লগইনে হার্ডওয়্যার MFA চালু করুন।