নাম: _____ তারিখ: _____ নম্বর: _____

পরিচয় চুরি প্রতিরোধ ও সম্পদ নিরাপত্তা গাইড

ক্রেডেনশিয়াল ফাঁস, MFA, ডার্ক ওয়েব মনিটরিং, ক্রেডিট ফ্রিজ সতর্কতা, সোশ্যাল ইঞ্জিনিয়ারিং

পরিচয় চুরি প্রতিরোধ: শিখন সংক্ষেপ

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 পরিচয় চুরি প্রতিরোধ ও প্রশমন বিষয়ে গাইড করবে। আপনি ক্রেডেনশিয়াল লিক, মাল্টি-ফ্যাক্টর প্রমাণীকরণ, ডার্ক ওয়েব পর্যবেক্ষণ, ক্রেডিট ফ্রিজ সতর্কতা এবং সোশ্যাল ইঞ্জিনিয়ারিং প্রতিরক্ষা 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/parichay-churi/

আপনার পরিচয় সুরক্ষা শেখার রোডম্যাপ

- ডার্ক ওয়েব ফোরামে ক্রেডেনশিয়াল প্রকাশের ঝুঁকি বুঝুন।
- মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) এবং ক্রেডিট ফ্রিজ সতর্কতা বাস্তবায়ন করুন।
- লক্ষ্যভিত্তিক সোশ্যাল ইঞ্জিনিয়ারিং প্রতারণার বিরুদ্ধে কর্পোরেট নিরাপত্তা প্রতিরক্ষা নকশা করুন।

পরিচয় চুরি গাইডের নির্দেশনা

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

পরিচয় চুরি প্রতিরোধ ও সম্পদ নিরাপত্তা (ভূমিকা)

পরিচয় চুরি ফাঁস হওয়া লগইন তথ্য ও দুর্বল লগইনের সুযোগ নিয়ে ব্যক্তিগত ও কর্পোরেট অ্যাকাউন্ট দখল করে। MFA, ক্রেডিট ফ্রিজ, ডার্ক ওয়েব স্ক্যানার এবং SPF/DKIM/DMARC কাঠামো চালু করা ডিজিটাল ছদ্মবেশ ধারণের বিরুদ্ধে একটি গুরুত্বপূর্ণ প্রতিরক্ষা গড়ে তোলে।

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

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. পরিচয় চোরেরা লগইন ক্রেডেনশিয়াল চুরির জন্য প্রধানত কোন পদ্ধতি ব্যবহার করে?**

- A. জাল পোর্টালে পাসওয়ার্ড দিতে ব্যবহারকারীদের প্রতারিত করে ভুয়া ইমেইল সতর্কতা পাঠানো
- B. ব্যবহারকারীর কর্পোরেট অফিসের কাছাকাছি রেডিও সম্প্রচার শোনা
- C. ব্যবহারকারীর স্থানীয় সার্ভার স্টোরেজ ড্রাইভ ডিফ্র্যাগমেন্ট করা
- D. বাহ্যিক নেটওয়ার্ক ব্যাকআপ কনফিগারেশন বিচ্ছিন্ন করা

2 **2. কোন নিরাপত্তা নিয়ন্ত্রণ ক্রেডেনশিয়াল লিকের বিরুদ্ধে সবচেয়ে শক্তিশালী প্রতিরক্ষা দেয়?**

- A. হার্ডওয়্যার কী ব্যবহার করে মাল্টি-ফ্যাক্টর অথেন্টিকেশন
- B. ব্রাউজারের ডিফল্ট ফরম্যাট ব্যবহার করে দীর্ঘ পাসওয়ার্ড তৈরি করা
- C. প্রতি ছয় মাসে ইমেইল ইউজারনেম পরিবর্তন করা
- D. সংরক্ষিত কুকি ট্র্যাকিং ব্রাউজার ইতিহাস মুছে ফেলা

3 **3. ক্রেডিট ফ্রিজিং কী বোঝায়?**

- A. চোরেরা অননুমোদিত ঋণ খুলতে না পারে সেজন্য ক্রেডিট রিপোর্ট লক করা
- B. ডেটাবেস থেকে ব্যাংক অ্যাকাউন্টের লেনদেনের ইতিহাস মুছে ফেলা
- C. স্ক্যানারে ক্রেডিট কার্ডের ম্যাগনেটিক সোয়াইপ রিডার বন্ধ করা
- D. স্থানীয় ডাটাবেস হার্ড ড্রাইভকে অ্যাট-রেস্ট এনক্রিপ্ট করা

4 **4. ডার্ক ওয়েব মনিটরিং কেন উপযোগী?**

- A. অবৈধ ডেটাবেসে ব্যবহারকারীর ফাঁস হওয়া ক্রেডেনশিয়াল দেখা গেলে এটি তাদের সতর্ক করে
- B. এটি ভার্চুয়াল স্যান্ডবক্সে সক্রিয় ম্যালওয়্যার চলা প্রতিরোধ করে
- C. এটি ভার্চুয়াল নেটওয়ার্কে ব্রাউজারের রাউটিং গতি বাড়ায়
- D. এটি ব্যাকএন্ড ডাটাবেস SQL ইনজেকশন প্রবেশ প্রচেষ্টা ব্লক করে

5 **5. সোশ্যাল ইঞ্জিনিয়ারিং বলতে কী বোঝায়?**

- A. মানুষকে প্রভাবিত করে স্বেচ্ছায় গোপন ক্রেডেনশিয়াল প্রকাশ করানো
- B. সক্রিয় নিরাপত্তা এক্সপ্লয়েটের জন্য কর্পোরেট সার্ভার পোর্ট স্ক্যান করা
- C. সিস্টেম ডেটাবেস ফাইল অফলাইন হার্ড ড্রাইভে ব্যাকআপ করা
- D. তিনটি এনক্রিপ্টেড অনিয়ন নোডের মধ্য দিয়ে নেটওয়ার্ক প্যাকেট রাউট করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. পরিচয় চুরি শুধু অনলাইন ডিজিটাল অ্যাকাউন্টকে প্রভাবিত করে, ভৌত ডাকযোগাযোগকে নয়।

- ◯ সত্য
- ◯ মিথ্যা

7 প্রশ্ন 7

7. সব ব্যক্তিগত অ্যাকাউন্টে MFA কার্যকর করলে বেশির ভাগ ক্রেডেনশিয়াল-স্টাফিং বট আক্রমণ ব্লক হয়।

- ◯ সত্য
- ◯ মিথ্যা

8 প্রশ্ন 8

8. ক্রেডিট ফ্রিজ ক্রেডিট যাচাই ব্লক করে কিন্তু আপনাকে নিজের ব্যাংক অ্যাকাউন্টে প্রবেশ করতে বাধা দেয়।

- ◯ সত্য
- ◯ মিথ্যা

9 প্রশ্ন 9

9. পাসওয়ার্ড ম্যানেজার জাল ডোমেইনে পাসওয়ার্ড অটো-ফিল করতে অস্বীকার করে ব্যবহারকারীকে ফিশিং থেকে সুরক্ষা দেয়।

- ◯ সত্য
- ◯ মিথ্যা

10 প্রশ্ন 10

10. ফিশিং ইমেইল প্রায়ই জরুরি ভাষা ব্যবহার করে, যাতে আবেগতাড়িত ও তড়িঘড়ি সাড়া পাওয়া যায়।

- ◯ সত্য
- ◯ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

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

1. পরিচয় চোরেরা ব্যক্তিগত পাসওয়ার্ড ও ব্যবহারকারীর _____ লক্ষ্য করে।

2. ডেটাবেস লঙ্ঘনের বিষয়ে ব্যবহারকারীদের সতর্ক করলে ব্যক্তিগত অ্যাকাউন্টের _____ শনাক্ত হয়।

3. সাইন ইনের জন্য অস্থায়ী কোড চাওয়াকে বলা হয় _____ ।

4. চুরি হওয়া ডেটার জন্য হ্যাকার ফোরাম স্ক্যান করা হলো ডার্ক ওয়েব _____ ।

5. অননুমোদিত ক্রেডিট যাচাই ঠেকাতে ক্রেডিট _____ দরকার।

6. কর্মীদের ফিশিং-সচেতনতা প্রশিক্ষণ দিলে সক্রিয় নিরাপত্তা- _____ গড়ে ওঠে।

পরিভাষা শব্দভাণ্ডার

এমএফএ | জাল ওয়েবসাইট | তথ্য ফাঁস | নজরদারি | প্রতিরক্ষা | ফ্রিজ | লগইন তথ্য স্পুফিং

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

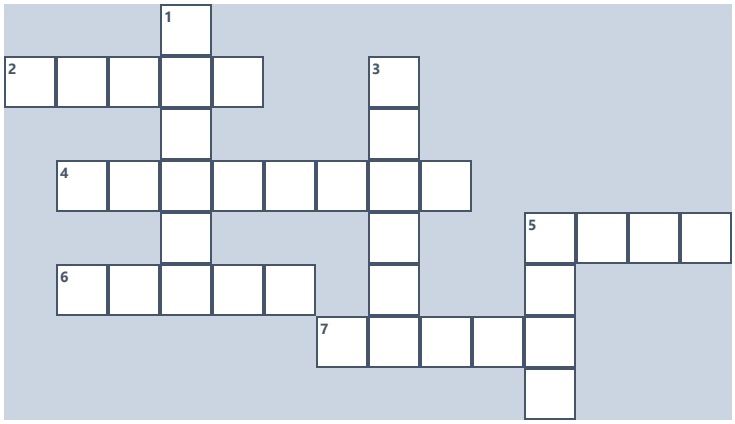
সংজ্ঞা মেলানো

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

☐	1. ক্রেডেনশিয়াল	A	অ্যাকাউন্ট লগইন সুরক্ষাকারী দ্বিতীয় যাচাইকরণ ধাপ (যেমন হার্ডওয়্যার কী)।
☐	2. ফাঁস	B	বৈধ প্রতিষ্ঠানের নকল করতে একটি ভুয়া ওয়েবসাইট বা ইমেইল তৈরি করা।
☐	3. MFA	C	প্রতারণামূলক ঋণের আবেদন ঠেকাতে ক্রেডিট ফাইলে প্রবেশ সীমিত করা।
☐	4. মনিটরিং	D	ব্যক্তিগত ব্যবহারকারীর রেকর্ডসংবলিত প্রাইভেট ডেটাবেসের অননুমোদিত প্রকাশ।
☐	5. ফ্রিজ	E	পরিচয় চুরির বিরুদ্ধে সুরক্ষার জন্য ব্যবহৃত প্রশিক্ষণ ও প্রযুক্তিগত নিয়ন্ত্রণ।
☐	6. প্রতিরক্ষা	F	ব্যবহারকারীদের ক্রেডেনশিয়াল দিয়ে দিতে প্রতারিত করতে ভুয়া বার্তা পাঠানো।
☐	7. স্পুফিং	G	চুরি যাওয়া কর্পোরেট ডেটার জন্য অনলাইন ফোরাম ও হ্যাকার চ্যানেল স্ক্যান করা।
☐	8. ফিশিং	H	ডিজিটাল পরিচয় প্রমাণীকরণে ব্যবহৃত ইউজারনেম, পাসওয়ার্ড ও প্রাইভেট টোকেন।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

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



পাশাপাশি

2. অ্যাকাউন্ট লগইন সুরক্ষা দেওয়া দ্বিতীয় যাচাই-ধাপ (যেমন হার্ডওয়্যার কী) (5)

4. বৈধ প্রতিষ্ঠানের অনুকরণে নকল ওয়েবসাইট বা ইমেইল তৈরি (8)

5. লোভ বা ভয় দেখিয়ে ঠকানোর কৌশল (4)

6. চুরি হওয়া কর্পোরেট ডেটার জন্য অনলাইন ফোরাম ও হ্যাকার-চ্যানেল স্ক্যান করা (5)

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

উপর-নিচ

1. কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6)

3. লগইন তথ্য হাতিয়ে নিতে ব্যবহারকারীকে ঠকানো প্রতারণামূলক বার্তা (6)

5. পরিচয় চুরি থেকে সুরক্ষায় ব্যবহৃত প্রশিক্ষণ ও কারিগরি নিয়ন্ত্রণ (4)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

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

পাশাপাশি

2 পাশাপাশি: অ্যাকাউন্ট লগইন সুরক্ষা দেওয়া দ্বিতীয় যাচাই-ধাপ (যেমন হার্ডওয়্যার কী) (5 অক্ষর):

4 পাশাপাশি: বৈধ প্রতিষ্ঠানের অনুকরণে নকল ওয়েবসাইট বা ইমেইল তৈরি (8 অক্ষর):

5 পাশাপাশি: লোভ বা ভয় দেখিয়ে ঠকানোর কৌশল (4 অক্ষর):

6 পাশাপাশি: চুরি হওয়া কর্পোরেট ডেটার জন্য অনলাইন ফোরাম ও হ্যাকার-চ্যানেল স্ক্যান করা (5 অক্ষর):

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

উপর-নিচ

1 উপর-নিচ: কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6 অক্ষর):

3 উপর-নিচ: লগইন তথ্য হাতিয়ে নিতে ব্যবহারকারীকে ঠকানো প্রতারণামূলক বার্তা (6 অক্ষর):

5 উপর-নিচ: পরিচয় চুরি থেকে সুরক্ষায় ব্যবহৃত প্রশিক্ষণ ও কারিগরি নিয়ন্ত্রণ (4 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

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

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

পরিভাষা শব্দতালিকা

এমএফএ নজরদারি প্রতিরক্ষা জালওয়েবসাইট ফিশিংইমেইল ম্যালওয়্যার প্রতারণা সফটওয়্যার

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. এমএফএ

B. নজরদারি

C. প্রতিরক্ষা

D. জালওয়েবসাইট

E. ফিশিংইমেইল

F. ম্যালওয়্যার

G. প্রতারণা

H. সফটওয়্যার

সংজ্ঞা ও মিলের ঘর

1. কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম।
2. অ্যাকাউন্ট লগইন সুরক্ষা দেওয়া দ্বিতীয় যাচাই-ধাপ (যেমন হার্ডওয়্যার কী)।
3. লোভ বা ভয় দেখিয়ে ঠকানোর কৌশল।
4. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার।
5. বৈধ প্রতিষ্ঠানের অনুকরণে নকল ওয়েবসাইট বা ইমেইল তৈরি।
6. লগইন তথ্য হাতিয়ে নিতে ব্যবহারকারীকে ঠকানো প্রতারণামূলক বার্তা।
7. চুরি হওয়া কর্পোরেট ডেটার জন্য অনলাইন ফোরাম ও হ্যাকার-চ্যানেল স্ক্যান করা।
8. পরিচয় চুরি থেকে সুরক্ষায় ব্যবহৃত প্রশিক্ষণ ও কারিগরি নিয়ন্ত্রণ।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

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

1. **ফ এ এ এ ম**
2. **প্র র ক্ষা তি**
3. **ফি ই মে ল ই শিং**
4. **ণা র প্র তা**
5. **র রি ন দা জ**
6. **ই ট য়ে সা জা ব ল ও**
7. **য়্যা র ম্যা ও ল**
8. **ট র স য়্যা ও ফ**

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

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

1	আপনার পরিচয় চুরি হলে যা করবেন			
2	সোশ্যাল মিডিয়ায় যা শেয়ার করা উচিত নয়			
3	যা যা আপনি ব্যাকআপ করেন			
4	আপনার মানিব্যাগে থাকা কার্ড বা আইডি			
5	আপনার সুরক্ষিত রাখা উচিত এমন নথি			
6	ডেটা ফাঁসের পর যা করবেন			
7	সফটওয়্যার আপডেট করার কারণ			
8	পরিচয় চোর যে তথ্য চায়			
9	যেসব ডিভাইস হ্যাক হতে পারে			
10	যেসব জায়গা থেকে আপনার ডেটা ফাঁস হতে পারে			
11	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
12	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
13	আপনি কে তা প্রমাণ করার উপায়			
14	পরিচয় চুরির লক্ষণ			
15	ইমেইলে সতর্কতার লক্ষণ			

চেকপয়েন্ট 8: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: নির্বাহীর পরিচয় ছদ্মবেশ থেকে সুরক্ষা



পরিস্থিতি: একজন হাই-প্রোফাইল C-suite নির্বাহী ক্লায়েন্টদের সঙ্গে প্রতারণা করতে তাঁর ব্যক্তিগত ইমেইলের অনুকরণ করা টাইপো-স্কোয়াট ডোমেইন নামের লক্ষ্যবস্তু হয়েছেন। একটি ব্র্যান্ড সুরক্ষা পরিকল্পনা তৈরি করুন।

আলোচনার প্রশ্ন: ব্র্যান্ড স্পুফিংয়ের ঝুঁকি বিশ্লেষণ করুন এবং SPF/DKIM/DMARC ও প্রমাণীকরণ নিয়ন্ত্রণ বিস্তারিত বর্ণনা করুন।

কেস স্টাডি 2: কর্পোরেট ক্রেডেনশিয়ালের ডার্ক ওয়েবে উন্মোচন



পরিস্থিতি: একটি ডার্ক ওয়েব ডেটাবেস ডাম্পে একটি এন্টারপ্রাইজের সিস্টেম অ্যাডমিনিস্ট্রেটরদের কয়েকশো কর্পোরেট ক্রেডেনশিয়াল আছে। একটি প্রশমন কৌশল তৈরি করুন।

আলোচনার প্রশ্ন: ক্রেডেনশিয়াল পরিষ্কারের প্রক্রিয়ার রূপরেখা দিন এবং একটি পাসওয়ার্ড ম্যানেজার চালুর পরিকল্পনা 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

8	36	8	33	8		29	46	37	59	51		24	46	19	46	22	45	39

32	38	46	17	37	59		34	45	57	17	45	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: পরিচয় চুরি কী?

একটি অপরাধ, যেখানে আক্রমণকারী আর্থিক লাভের জন্য অন্যের ছদ্মবেশ ধারণ করতে ব্যক্তিগত রেকর্ড (যেমন পাসওয়ার্ড বা SSN) চুরি করে।

Q2: পরিচয় চুরির সবচেয়ে সাধারণ কারণ কী?

ফিশিং হলো পাসওয়ার্ড চুরির একটি প্রধান উপায়, যেখানে ব্যবহারকারীদের ভুলিয়ে জাল ও স্পুফ করা ওয়েবসাইটে নিয়ে যাওয়া হয়।

Q3: মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) কীভাবে পরিচয় সুরক্ষিত রাখে?

MFA-তে লগ ইন করতে দ্বিতীয় একটি প্রমাণ (যেমন হার্ডওয়্যার কী) লাগে, ফলে আক্রমণকারী আপনার পাসওয়ার্ড চুরি করলেও ঢুকতে পারে না।

Q4: ক্রেডিট ফ্রিজ কী?

ক্রেডিট ব্যুরোগুলোকে আপনার ক্রেডিট ফাইল শেয়ার করতে বাধা দেওয়া একটি বিনামূল্যের সেবা, যা চোরদের আপনার নামে নতুন ঋণ খোলা ঠেকায়। [2]

Q5: ডার্ক ওয়েব মনিটরিং কী?

হ্যাকার ফোরামে ফাঁস হওয়া ইমেইল, পাসওয়ার্ড ও ব্যক্তিগত রেকর্ড খুঁজে দেখা এবং আপনার ডেটা উন্মুক্ত হলে সতর্ক করা সফটওয়্যার।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: ক্রেডেনশিয়াল স্টাফিং বলতে কী বোঝায়?

ফাঁস হওয়া পাসওয়ার্ড তালিকা শত শত ওয়েবসাইটে পরীক্ষা করে সক্রিয় অ্যাকাউন্ট দখল করা স্বয়ংক্রিয় বট।

Q7: ইমেইল স্পুফিং কেন বিপজ্জনক?

এটি আক্রমণকারীদের ইমেইলে প্রেরকের নাম জাল করতে দেয়, ফলে ফিশিং বার্তাগুলো বিশ্বস্ত সহকর্মীদের কাছ থেকে এসেছে বলে মনে হয়।

Q8: পাসওয়ার্ড ম্যানেজার কীভাবে পরিচয় চুরি ঠেকায়?

এরা প্রতিটি অ্যাকাউন্টের জন্য জটিল, অনন্য পাসওয়ার্ড সংরক্ষণ করে এবং ভুয়া ফিশিং ডোমেইনে স্বয়ংক্রিয়ভাবে ক্রেডেনশিয়াল পূরণ করতে অস্বীকার করে।

Q9: স্পিয়ার ফিশিং কী?

প্রতারণার সম্ভাবনা বাড়াতে ভুক্তভোগীর নাম ও তথ্য ব্যবহার করে সাজানো একটি অত্যন্ত লক্ষ্যভিত্তিক ফিশিং আক্রমণ।

Q10: ক্রেডিট সতর্কতা ও ফ্রিজের মধ্যে পার্থক্য কী?

অ্যালার্ট ঋণদাতাদের অ্যাকাউন্ট খোলার আগে আপনার পরিচয় যাচাই করতে বলে, আর ফ্রিজ আপনার ক্রেডিট ফাইলে প্রবেশ সম্পূর্ণভাবে আটকে দেয়। [2]

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

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

Q1: সিম সোয়াপিং কীভাবে পরিচয় চুরির দিকে নিয়ে যায়?

আক্রমণকারীরা ক্যারিয়ার কর্মীদের প্ররোচিত করে ভুক্তভোগীর ফোন নম্বর নতুন SIM কার্ডে স্থানান্তর করায় এবং SMS-ভিত্তিক 2FA কোড হাইজ্যাক করে।

Q2: পরিচয় চুরি ঠেকাতে DMARC-এর ভূমিকা কী?

DMARC ডোমেইন মালিকদের স্পুফ করা ইমেল ইনবক্সে পৌঁছানো আটকাতে দেয়, ফলে কর্পোরেট ডোমেইনের নকল ইমেল বন্ধ হয়।

Q3: সিনথেটিক পরিচয় চুরি শনাক্ত করা কেন কঠিন?

চোরেরা আসল SSN-এর সঙ্গে ভুয়া নাম ও জন্মতারিখ মিলিয়ে একেবারে নতুন ক্রেডিট প্রোফাইল তৈরি করে, ফলে মৌলিক জালিয়াতি সতর্কতা এড়িয়ে যায়।

Q4: ডেটা ব্রোকাররা কীভাবে ব্যক্তিগত পরিচয়ের অপব্যবহার করে?

ব্রোকাররা প্রোফাইল ডসিয়ার তৈরি করতে পাবলিক রেকর্ড, ওয়েব আচরণ ও ক্রয়ের ইতিহাস সংগ্রহ করেন, যা ফাঁস বা বিক্রি হতে পারে।

Q5: SMS-ভিত্তিক MFA কেন দুর্বল বলে বিবেচিত?

SMS ট্রাফিক ইন্টারসেপশন, ফিশিং এবং ক্যারিয়ার-স্তরের SIM-সোয়াপিং আক্রমণের ঝুঁকিতে থাকে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

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

Q6: ক্রেডিট ফাইল লক কী?

ফ্রিজের মতো একটি বাণিজ্যিক সেবা, যা ব্যবহারকারীদের মোবাইল অ্যাপের মাধ্যমে তাৎক্ষণিকভাবে ক্রেডিট ফাইল আনলক বা লক করার সুযোগ দেয়।

Q7: কর্পোরেট ডেটা ফাঁস কীভাবে পরিচয় চুরিকে উসকে দেয়?

ফাঁস হওয়া ডাটাবেস লক্ষ লক্ষ প্লেইন ক্রেডেনশিয়াল প্রকাশ করে দেয়, ফলে চোরেরা লক্ষ্যভিত্তিক পরিচয় জালিয়াতি চালানোর কাঁচা তথ্য পেয়ে যায়।

Q8: সোশ্যাল মিডিয়ায় অতিরিক্ত তথ্য শেয়ারের ঝুঁকি কী?

পোষা প্রাণীর নাম, জন্মস্থান ও মায়ের বিয়ের আগের পদবি প্রকাশ্যে শেয়ার করলে চোরেরা অ্যাকাউন্ট পুনরুদ্ধারের সাধারণ প্রশ্নের উত্তর পেয়ে যায়।

Q9: বায়োমেট্রিক লগইন কীভাবে পরিচয় প্রোফাইল সুরক্ষিত রাখে?

বায়োমেট্রিক্স লগইনকে আঙুলের ছাপ বা মুখের মতো বৈশিষ্ট্যের সঙ্গে যুক্ত করে; ডিভাইসে রাখা হলে সেগুলো চুরি করা কঠিন, কিন্তু সংরক্ষিত বায়োমেট্রিক ডেটা ফাঁস হতে পারে।

Q10: Red Flags Rule কীভাবে পরিচয় চুরির বিরুদ্ধে লড়াই করে?

একটি ফেডারেল বিধান, যা আর্থিক প্রতিষ্ঠানগুলোকে পরিচয় চুরির সতর্কতা সংকেত শনাক্ত ও তার জবাব দেওয়ার জন্য লিখিত কর্মসূচি তৈরি করতে বাধ্য করে।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

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

1. নিরাপত্তা ইনসাইট

FTC পরিচালিত IdentityTheft.gov মার্কিন ভুক্তভোগীদের পরিচয় চুরির ঘটনা জানাতে এবং ব্যক্তিগত পুনরুদ্ধার পরিকল্পনা পেতে সাহায্য করে। [1]

2. নিরাপত্তা ইনসাইট

হার্ডওয়্যার সিকিউরিটি কী ফিশিং-প্রতিরোধী MFA, যা CISA-র সুপারিশ করা সবচেয়ে শক্তিশালী ধরনের MFA। [4]

3. নিরাপত্তা ইনসাইট

ফাঁস হওয়া পাসওয়ার্ড ডেটা ফাঁসের একটি সাধারণ প্রবেশপথ, যা পরবর্তীকালে পরিচয় জালিয়াতিতে ইন্ধন জোগায়।

4. নিরাপত্তা ইনসাইট

ফেডারেল আইনে ক্রেডিট ফ্রিজ বিনামূল্যে, যা আনলক না করা পর্যন্ত ঋণদাতাদের ক্রেডিট ফাইল যাচাই করতে বাধা দেয়। [2]

5. নিরাপত্তা ইনসাইট

DMARC ডোমেইন মালিকদের মেইল সার্ভারকে বলতে দেয় যাচাইয়ে ব্যর্থ স্পুফ করা ইমেল প্রত্যাখ্যান বা কোয়ারেন্টাইন করতে। [7]

6. নিরাপত্তা ইনসাইট

SIM সোয়াপিংয়ের মাধ্যমে হ্যাকাররা ব্যাংকিং পোর্টালে SMS-ভিত্তিক টু-ফ্যাক্টর অথেনটিকেশন এড়াতে পারে।

7. সিকিউরিটি ইনসাইট

সিনথেটিক পরিচয় প্রতারণায় আসল ও ভুয়া তথ্য মেশানো হয়, ফলে ঋণদাতাদের পক্ষে তা শনাক্ত করা কঠিন।

8. সিকিউরিটি ইনসাইট

অনেকে একই পাসওয়ার্ড একাধিক অনলাইন অ্যাকাউন্টে ব্যবহার করে, তাই একটি ডেটা ভঙ্গে কয়েকটি অ্যাকাউন্টই ঝুঁকিতে পড়তে পারে।

9. সিকিউরিটি ইনসাইট

ডেটা ব্রোকাররা বিপুল সংখ্যক ভোক্তার বিস্তারিত তথ্যভান্ডার তৈরি করে, যা কেন্দ্রীভূত গোপনীয়তা ঝুঁকি সৃষ্টি করে।

10. নিরাপত্তা ইনসাইট

পরিচয় চুরি থেকে পুনরুদ্ধারে কয়েক মাসের কাজ লাগতে পারে, যেমন অনুমোদনহীন চার্জ নিয়ে আপত্তি জানানো ও ক্রেডিট রিপোর্ট ঠিক করা।

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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

পরিচয় চোরেরা লগইন ক্রেডেনশিয়াল চুরির জন্য প্রধানত কোন পদ্ধতি ব্যবহার করে? → জাল পোর্টালে পাসওয়ার্ড দিতে ব্যবহারকারীদের প্রতারিত করে ভুয়া ইমেইল সতর্কতা পাঠানো

2 প্রশ্ন 2

সঠিক উত্তর: A

শিক্ষণ নোট

কোন নিরাপত্তা নিয়ন্ত্রণ ক্রেডেনশিয়াল লিকের বিরুদ্ধে সবচেয়ে শক্তিশালী প্রতিরক্ষা দেয়? → হার্ডওয়্যার কী ব্যবহার করে মাল্টি-ফ্যাক্টর অথেন্টিকেশন

3 প্রশ্ন 3

সঠিক উত্তর: A

শিক্ষণ নোট

ক্রেডিট ফ্রিজিং কী বোঝায়? → চোরেরা অননুমোদিত ঋণ খুলতে না পারে সেজন্য ক্রেডিট রিপোর্ট লক করা

4 প্রশ্ন 4

সঠিক উত্তর: A

শিক্ষণ নোট

ডার্ক ওয়েব মনিটরিং কেন উপযোগী? → অবৈধ ডেটাবেসে ব্যবহারকারীর ফাঁস হওয়া ক্রেডেনশিয়াল দেখা গেলে এটি তাদের সতর্ক করে

5 প্রশ্ন 5

সঠিক উত্তর: A

শিক্ষণ নোট

সোশ্যাল ইঞ্জিনিয়ারিং বলতে কী বোঝায়? → মানুষকে প্রভাবিত করে স্বেচ্ছায় গোপন ক্রেডেনশিয়াল প্রকাশ করানো

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

পরিচয় চুরি অফলাইনেও শুরু হতে পারে, যেমন চুরি হওয়া ডাক বা নথি থেকে।

7 প্রশ্ন 7 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সব ব্যক্তিগত অ্যাকাউন্টে MFA কার্যকর করলে বেশির ভাগ ক্রেডেনশিয়াল-স্টাফিং বট আক্রমণ ব্লক হয়।

8 প্রশ্ন 8 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

ক্রেডিট ফ্রিজ নতুন ক্রেডিট যাচাই বন্ধ করে, কিন্তু আপনার বিদ্যমান অ্যাকাউন্টে প্রভাব ফেলে না।

9 প্রশ্ন 9 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

পাসওয়ার্ড ম্যানেজার জাল ডোমেইনে পাসওয়ার্ড অটো-ফিল করতে অস্বীকার করে ব্যবহারকারীকে ফিশিং থেকে সুরক্ষা দেয়।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

ফিশিং ইমেইল প্রায়ই জরুরি ভাষা ব্যবহার করে, যাতে আবেগতাড়িত ও তড়িঘড়ি সাড়া পাওয়া যায়।

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

H 1. ক্রেডেনশিয়াল	D 2. ফাঁস	A 3. MFA	G 4. মনিটরিং
C 5. ফ্রিজ	E 6. প্রতিরক্ষা	B 7. স্পুফিং	F 8. ফিশিং

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 লগইন তথ্য	2 তথ্য ফাঁস	3 এমএফএ	4 নজরদারি
5 ফ্রিজ	6 প্রতিরক্ষা		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 H – সফটওয়্যার	2 A – এমএফএ	3 G – প্রতারণা	4 F – ম্যালওয়্যার
5 D – জালওয়েবসাইট	6 E – ফিশিংইমেইল	7 B – নজরদারি	8 C – প্রতিরক্ষা

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা ক্রেডেনশিয়াল, ফাঁস ও MFA 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।

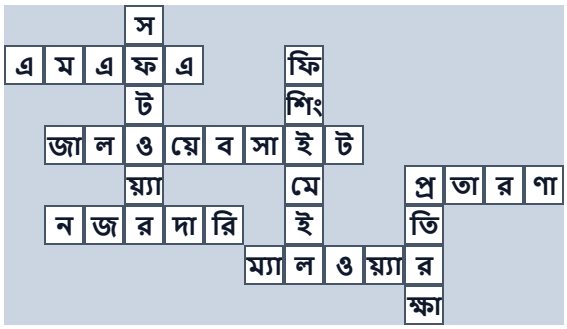
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

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

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

2 পাশাপাশি: এমএফএ অ্যাকাউন্ট লগইন সুরক্ষা দেওয়া দ্বিতীয় যাচাই-ধাপ (যেমন হার্ডওয়্যার কী) (5 অক্ষর)

4 পাশাপাশি: জালওয়েবসাইট বৈধ প্রতিষ্ঠানের অনুকরণে নকল ওয়েবসাইট বা ইমেইল তৈরি (8 অক্ষর)

5 পাশাপাশি: প্রতারণা লোভ বা ভয় দেখিয়ে ঠকানোর কৌশল (4 অক্ষর)

6 পাশাপাশি: নজরদারি চুরি হওয়া কর্পোরেট ডেটার জন্য অনলাইন ফোরাম ও হ্যাকার-চ্যানেল স্ক্যান করা (5 অক্ষর)

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

উপর-নিচ

1 উপর-নিচ: সফটওয়্যার কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6 অক্ষর)

3 উপর-নিচ: ফিশিংইমেইল লগইন তথ্য হাতিয়ে নিতে ব্যবহারকারীকে ঠকানো প্রতারণামূলক বার্তা (6 অক্ষর)

5 উপর-নিচ: প্রতিরক্ষা পরিচয় চুরি থেকে সুরক্ষায় ব্যবহৃত প্রশিক্ষণ ও কারিগরি নিয়ন্ত্রণ (4 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

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

শব্দ সাজানোর উত্তরমালা

1. ফএএএম — **এমএফএ**
2. প্ররক্ষাতি — **প্রতিরক্ষা**
3. ফিইমেলইশিং — **ফিশিংইমেইল**
4. ণারপ্রতা — **প্রতারণা**
5. ররিনদাজ — **নজরদারি**
6. ইটয়েসাজাবলও — **জালওয়েবসাইট**
7. য়্যারম্যাওল — **ম্যালওয়্যার**
8. টরসয়্যাওফ — **সফটওয়্যার**

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"এমএফএ দিয়ে ডিজিটাল পরিচয় বাঁচান"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: নির্বাহীর পরিচয় ছদ্মবেশ থেকে সুরক্ষা

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একজন হাই-প্রোফাইল C-suite নির্বাহী ক্লায়েন্টদের সঙ্গে প্রতারণা করতে তার ব্যক্তিগত ইমেলের অনুকরণ করা টাইপো-স্কোয়াট করা ডোমেইন নামের লক্ষ্যবস্তু হয়েছেন। একটি ব্র্যান্ড সুরক্ষা পরিকল্পনা তৈরি করুন।
- প্রস্তাবিত কৌশল ও সমাধান: নির্বাহীর নামের সব প্রচলিত বানান-বৈচিত্র্য নিবন্ধন করুন। ডোমেইন স্পুফিং ঠেকাতে ইমেল অথেনটিকেশন প্রোটোকল (DMARC, DKIM, SPF) প্রয়োগ করুন। সব C-suite কর্পোরেট লগইনে হার্ডওয়্যার MFA বাধ্যতামূলক করুন।

B কেস স্টাডি 2: কর্পোরেট ক্রেডেনশিয়ালের ডার্ক ওয়েবে উন্মোচন

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি ডার্ক ওয়েব ডেটাবেস ডাম্পে একটি এন্টারপ্রাইজের সিস্টেম অ্যাডমিনিস্ট্রেটরদের কয়েকশ কর্পোরেট ক্রেডেনশিয়াল রয়েছে। একটি প্রশমন কৌশল ডিজাইন করুন।
- প্রস্তাবিত কৌশল ও সমাধান: কোম্পানিজুড়ে পাসওয়ার্ড রিসেট করুন। এন্টারপ্রাইজ পাসওয়ার্ড ম্যানেজার ব্যবহার বাধ্যতামূলক করুন। সব সিস্টেম পোর্টালে MFA কার্যকর করুন এবং ধারাবাহিক স্বয়ংক্রিয় ডার্ক ওয়েব মনিটরিং সতর্কবার্তা চালু করুন।