নাম: _____ তারিখ: _____ নম্বর: _____

VPN কী ওয়ার্কশিট

নেটওয়ার্ক প্রোটোকল, টানেলিং ও নিরাপত্তা নিয়ন্ত্রণের ব্যবহারিক অনুশীলন।

VPN শিক্ষণ সারসংক্ষেপ

শিক্ষার্থী
শিক্ষার্থী স্ট্যাটাস
নেটওয়ার্ক ডিফেন্ডার ট্র্যাক

নিরাপদ
সংযোগের অবস্থা
ডেটা প্যাকেট সুরক্ষিত রাখা

সক্রিয়
লিক সুরক্ষা
DNS ও IPv6 লিক সুরক্ষা

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)-এর মৌলিক নীতি বিষয়ে গাইড করবে। আপনি জানবেন এনক্রিপ্টেড টানেল কীভাবে আপনার ডেটা সুরক্ষিত করে, নেটওয়ার্ক প্রোটোকল কীভাবে কাজ করে এবং গোপনীয়তা লিক কীভাবে শনাক্ত ও প্রশমিত করবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: VPN-এর ধারণা ও প্রোটোকলে 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 VPN গাইড খুলুন

URL: https://www.vpn.com/bn/vpn/

আপনার VPN শেখার রোডম্যাপ

- ডেটা টানেলিং ও এনক্যাপসুলেশনের ধারণা ব্যাখ্যা করুন।
- স্ট্যান্ডার্ড প্রোটোকল কনফিগারেশন ও এনক্রিপশন পদ্ধতি শনাক্ত করুন।
- ভার্চুয়াল প্রাইভেট নেটওয়ার্কে সার্ভার ও IP মাস্কিংয়ের ভূমিকা বিশ্লেষণ করুন।
- ISP কীভাবে ব্রাউজিং ট্র্যাক করে এবং VPN কীভাবে তা ঠেকায় তা বুঝুন।
- ভার্চুয়াল নেটওয়ার্ক টপোলজির কার্যকর সীমানার মধ্যে পার্থক্য করুন।

VPN কী 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। কেস স্টাডি অংশের বাস্তব পরিস্থিতিতে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

VPN কী? (ভূমিকা)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক কেবল একটি প্রাইভেসি সুইচ নয়। এটি একটি এনক্রিপ্টেড টানেল, যা আপনার ইন্টারনেট ট্রাফিককে একটি রিমোট সার্ভারের মধ্য দিয়ে পাঠায়। এতে আপনার IP অ্যাড্রেস লুকায়, আপনার ISP আপনার অনলাইন কার্যকলাপের লগ জমাতে পারে না এবং পাবলিক নেটওয়ার্কে আপনার ডেটা সুরক্ষিত থাকে। ডিজিটাল নিরাপত্তা বজায় রাখতে পরিভাষাগুলো বোঝা অপরিহার্য।

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

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. ভার্চুয়াল প্রাইভেট নেটওয়ার্কের (VPN) প্রধান কাজ কী?**

- A. ইন্টারনেট ব্রাউজারের রেন্ডারিং গতি বাড়াতে
- B. ডেটা প্যাকেট এনক্রিপ্ট করতে এবং আপনার পাবলিক IP আড়াল করতে
- C. ওয়েবসাইটের কুকি ডাটাবেস স্থানীয়ভাবে সংরক্ষণ করতে
- D. আপনার ভৌত কম্পিউটার হার্ডওয়্যার প্রতিস্থাপন করতে

2 **2. VPN-এর প্রেক্ষাপটে নেটওয়ার্ক টানেলিং কী?**

- A. ডুপ্লিকেট নেটওয়ার্ক লগ ফাইল মুছে ফেলা
- B. স্থানীয় ডেটাবেস স্টোরেজ ফাইল ইনস্টল করা
- C. অন্য স্থানীয় কম্পিউটারের সঙ্গে ফাইল শেয়ার করা
- D. একটি নেটওয়ার্ক প্যাকেটকে আরেকটি নিরাপদ প্যাকেটের ভেতরে মুড়ে দেওয়া

3 **3. VPN ট্রাফিক সুরক্ষায় কোন এনক্রিপশন স্ট্যান্ডার্ড ব্যাপকভাবে ব্যবহৃত হয়?**

- A. পুরোনো DES এনক্রিপশন
- B. আধুনিক AES-256 স্ট্যান্ডার্ড
- C. প্লেইনটেক্সট base64 এনকোডিং
- D. স্ট্যান্ডার্ড rot13 সাইফারিং

4 **4. VPN আপনার নেটওয়ার্ক ট্রাফিকের কোন অংশ এনক্রিপ্ট করে?**

- A. শুধু স্থানীয় ডিভাইসের নেটওয়ার্ক প্রিন্ট কাজ
- B. ফিজিক্যাল ইথারনেট ক্যাবলের রাউটিং পথ
- C. নেটওয়ার্ক প্যাকেটের সম্পূর্ণ ডেটা পেলোড অংশ
- D. শুধু আপনার ওয়েব ব্রাউজারের সার্চ ইতিহাস

5 **5. নেটওয়ার্কিংয়ে 'এনক্রিপশন' শব্দটির অর্থ কী?**

- A. প্লেইনটেক্সট ডেটাকে অপাঠ্য সাইফারটেক্সটে রূপান্তর করা
- B. পুরোনো যোগাযোগ রেকর্ড মুছে ফেলা
- C. আপনার স্থানীয় ব্যান্ডউইথ গতিসীমা বাড়ানো
- D. ডাটাবেস প্রবেশ কী প্রকাশ্যে শেয়ার করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. পাবলিক Wi-Fi-তে স্থানীয় আড়ি পাতা ঠেকাতে VPN আপনার ট্রাফিক এনক্রিপ্ট করে।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. VPN আপনার রাউটার ডিভাইসের হার্ডওয়্যার কনফিগারেশন ভৌতভাবে বদলে দেয়।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. টানেলিং প্রোটোকল ডেটা প্যাকেটকে এনক্রিপ্টেড ট্রান্সপোর্ট স্তরে মুড়ে দেয়।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. সিমেট্রিক এনক্রিপশনে ট্রাফিক এনক্রিপ্ট ও ডিক্রিপ্ট করতে একই কী ব্যবহৃত হয়।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. VPN ব্যবহার আপনার ইন্টারনেট সংযোগকে অফলাইন বিদ্যুৎ বিভ্রাট থেকে ভৌতভাবে অক্ষত রাখে।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

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

1. ট্র্যাফিক সুরক্ষিত করতে ভিপিএন আপনার ডেটা প্যাকেটকে অন্য একটি প্রোটোকলের ভেতরে মুড়ে দেয়, এই প্রক্রিয়াকে বলা হয় _____ ।

2. স্ট্রিমিংয়ের সময় ডাউনলোড গতি ধীর হলে তার কারণ হতে পারে সীমিত নেটওয়ার্ক _____ ।

3. শুধু নির্দিষ্ট একটি দেশে পাওয়া যায় এমন স্ট্রিমিং সেবা বৈশ্বিক ব্যবহারকারীদের সীমিত করতে একটি _____ ব্যবহার করে।

4. এনক্রিপশন ও সংযোগের প্যারামিটার নির্ধারণকারী সংযোগ-নিয়মাবলিকে বলা হয় ভিপিএন _____ ।

5. আপনার কম্পিউটার নেটওয়ার্ক ট্র্যাফিক পর্যবেক্ষণ ও অনিরাপদ সংযোগ আটকাতে একটি স্থানীয় _____ ব্যবহার করে।

6. ভিপিএনে সংযোগ করলে আপনার পাবলিক আইপি লুকাতে আপনার ডেটা একটি দূরবর্তী _____ দিয়ে পাঠানো হয়।

পরিভাষা শব্দভাণ্ডার

এনক্রিপশন | জিও-ব্লক | টানেলিং | নজরদারি | প্রোটোকল | ফায়ারওয়াল | ব্যান্ডউইথ | সার্ভার

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নেটওয়ার্ক ধারণা মিলান

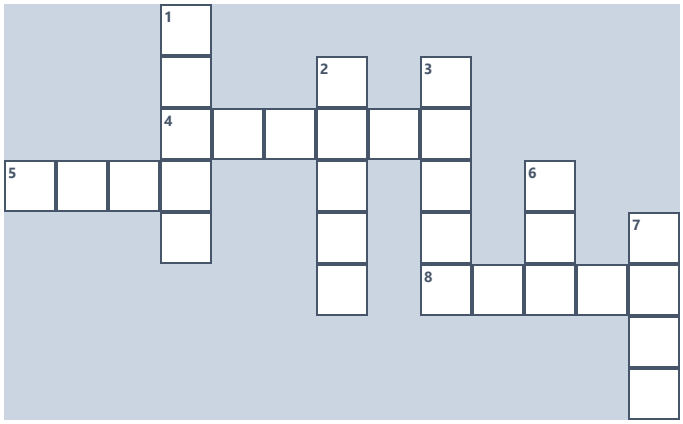
সংজ্ঞা মেলানো

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

____	1. টানেলিং	A	আপনার ট্রাফিক রাউট করা ও IP আড়াল করা একটি রিমোট কম্পিউটার।
____	2. প্রটোকল	B	যে ইন্টারনেট সেবা প্রদানকারী আপনার ট্রাফিক বহন করে এবং এনক্রিপ্ট না করা কার্যকলাপ দেখতে পারে।
____	3. ব্যান্ডউইথ	C	ভৌত অবস্থানের ভিত্তিতে ওয়েব অ্যাক্সেস আটকে দেওয়া একটি নিষেধাজ্ঞা।
____	4. সার্ভার	D	অননুমোদিত ট্রাফিক পর্যবেক্ষণ ও ব্লক করা একটি নিরাপত্তা ব্যবস্থা।
____	5. জিওব্লক	E	নেটওয়ার্কে ডেটা কীভাবে পাঠানো হবে তা নির্ধারণকারী নিয়মের একটি সংকলন।
____	6. ফায়ারওয়াল	F	ট্র্যাকিং বা জনসমক্ষে নজরদারি থেকে মুক্ত থাকার অবস্থা।
____	7. প্রাইভেসি	G	একটি সংযোগের মধ্য দিয়ে ডেটা স্থানান্তরের সর্বোচ্চ হার।
____	8. ISP	H	নিরাপদ ট্রানজিটের জন্য ডেটা প্যাকেটকে অন্য একটি প্যাকেটের ভেতরে মুড়ে দেওয়া।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

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



পাশাপাশি

4. তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি (6)

5. ফোন বা কম্পিউটারের মতো ব্যবহারযোগ্য যন্ত্র (4)

8. অনলাইন কার্যকলাপের ওপর গোপনে নজর রাখা (5)

উপর-নিচ

1. ইন্টারনেট সেবাদাতা, যারা এনক্রিপ্ট না করলে আপনার ট্র্যাফিক লগ করে (5)

2. ট্র্যাকিং বা জনসাধারণের নজরদারি থেকে মুক্ত থাকার অবস্থা (5)

3. ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5)

6. আপনার ট্র্যাফিক রাউট করে ও আইপি আড়াল করা দূরবর্তী কম্পিউটার (3)

7. ব্যবহারকারীকে শনাক্তকারী তথ্য (4)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

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

পাশাপাশি

4 পাশাপাশি: তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি (6 অক্ষর):

5 পাশাপাশি: ফোন বা কম্পিউটারের মতো ব্যবহারযোগ্য যন্ত্র (4 অক্ষর):

8 পাশাপাশি: অনলাইন কার্যকলাপের ওপর গোপনে নজর রাখা (5 অক্ষর):

উপর-নিচ

1 উপর-নিচ: ইন্টারনেট সেবাদাতা, যারা এনক্রিপ্ট না করলে আপনার ট্র্যাফিক লগ করে (5 অক্ষর):

2 উপর-নিচ: ট্র্যাকিং বা জনসাধারণের নজরদারি থেকে মুক্ত থাকার অবস্থা (5 অক্ষর):

3 উপর-নিচ: ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5 অক্ষর):

6 উপর-নিচ: আপনার ট্র্যাফিক রাউট করে ও আইপি আড়াল করা দূরবর্তী কম্পিউটার (3 অক্ষর):

7 উপর-নিচ: ব্যবহারকারীকে শনাক্তকারী তথ্য (4 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

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

ই ট লে ছ ণ লে তা বি নি ঘ ল মি কে ভ ড
রা ন র ঈ তি গ ই সে প ভ মা ণ জে ঘ চ
ই ই হ ণ দ নে স ঝ কা রি জ রা ফ ঘ উ
সে লা জি আ ড প পা ধ দ জি চ কি না লি ই
রে ন ফ চ ব এ দি শ জা রা দে য় ট মে র
ক অ সি দ ঠ ন হ আ সা শ মে সা র্ভা র দে
রা কি ঋ তে না ক্রি নে ছ ই য প উ অ উ ঋ
রি মা বা য ফ প বা ম দে এ তি ভ ঘ রে ষ
দা ফ ঘ দ হ শ স ভ রি মি স ঢ ষ ষ রি
র সি না তি তা ন ড ঊ নি রা কি পি থ সে ঊ
জ গো প নী য় তা লি গ নি জা পি ঋ জি লি ডি
ন ট ভ ণ জে গ স ঘ রে দি মি ঋ পা ভা উ
অ জে কা গ ম আ ঘ কি ঘ ঝ ণ ধ ই গ সি
রি শ ছ দ সে জি নি ঝ রে পে জ স আ আ রে
মা স মে তি দে রি ফ সি তি সে খ স বে উ ট

পরিভাষা শব্দতালিকা

সার্ভার গোপনীয়তা আইএসপি অনলাইন ডিভাইস এনক্রিপশন নজরদারি পরিচয়

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. সার্ভার

B. গোপনীয়তা

C. আইএসপি

D. অনলাইন

E. এনক্রিপশন

F. নজরদারি

G. পরিচয়

H. ডিভাইস

সংজ্ঞা ও মিলের ঘর

1. ট্র্যাকিং বা জনসাধারণের নজরদারি থেকে মুক্ত থাকার অবস্থা।
2. তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি।
3. অনলাইন কার্যকলাপের ওপর গোপনে নজর রাখা।
4. ব্যবহারকারীকে শনাক্তকারী তথ্য।
5. ফোন বা কম্পিউটারের মতো ব্যবহারযোগ্য যন্ত্র।
6. আপনার ট্র্যাফিক রাউট করে ও আইপি আড়াল করা দূরবর্তী কম্পিউটার।
7. ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা।
8. ইন্টারনেট সেবাদাতা, যারা এনক্রিপ্ট না করলে আপনার ট্র্যাফিক লগ করে।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

VPN-এর মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর পূরণযোগ্য ইনপুট বাক্সে লিখুন।

1. ভা র সা
2. আ পি স এ ই
3. এ ক্রি প ন শ ন
4. য় চ প রি
5. নী তা গো য় প
6. ই অ লা ন ন
7. দা রি ন র জ
8. ডি স ই ভা

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

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

1	একটি IP অ্যাড্রেস যা যা প্রকাশ করতে পারে			
2	VPN নিয়ে প্রচলিত ভুল ধারণা			
3	ইন্টারনেটজুড়ে চলাচল করে এমন জিনিস			
4	একজন ভালো VPN প্রদানকারীর প্রতিশ্রুতি			
5	যেসব গোপন তথ্য আপনি এনক্রিপ্ট করবেন			
6	যেসব জিনিস থেকে VPN আপনাকে সুরক্ষা দিতে পারে না			
7	ভুয়া Wi-Fi নেটওয়ার্ক চেনার উপায়			
8	গোপনীয়তার সঙ্গে সম্পর্কিত শব্দ			
9	যেসব ডিভাইসে VPN ব্যবহার করা যায়			
10	'Connect' চাপলে যা যা ঘটে			
11	যেসব জায়গায় আপনি VPN ব্যবহার করবেন			
12	ভ্রমণের সময় VPN ব্যবহারের কারণ			
13	বাস্তব জীবনে টানেলের মতো দেখতে জিনিস			
14	এই ওয়ার্কশিটের যে শব্দগুলো আপনি মনে রাখতে চান			
15	একটি শিশুকে VPN বোঝানোর শব্দ			

চেকপয়েন্ট 8: VPN কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

সারাহ (ক্যাফের শিক্ষার্থী)

👱 "হ্যালো! আমি Coffee & Bytes-এ বসে আছি। এখানে 'Free_Wi-Fi_No_Password' নামে একটি অনিরাপদ পাবলিক নেটওয়ার্ক আছে। আমি আমার স্কুলের ইমেইলে লগ ইন করে অ্যাসাইনমেন্ট আপলোড করতে চাই, কিন্তু হ্যাকারদের নিয়ে চিন্তিত। VPN ছাড়া এই নেটওয়ার্ক ব্যবহার করলে কী কী ঝুঁকি আছে, আর VPN কীভাবে আমার ডেটা সুরক্ষিত করে?"

অ্যালেক্স (ভ্রমণকারী শিক্ষার্থী)

👱 "ইশ! আমি একটি প্রকল্পের জন্য বিদেশে ভ্রমণ করছি এবং আমার নিজের দেশের একটি সার্ভারে হোস্ট করা জীববিজ্ঞানের ডকুমেন্টারি দেখার চেষ্টা করছি। কিন্তু সাইট বলছে 'এই ভিডিও আপনার বর্তমান অবস্থানে উপলব্ধ নয়।' আমি কেন ব্লক হচ্ছি, আর VPN কীভাবে আমাকে এটি দেখতে সাহায্য করতে পারে?"

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

VPN আপনার ট্রাফিক সুরক্ষিত রাখতে এনক্রিপ্ট করে। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে সাইবার নিরাপত্তা 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

31	46	38	45	32	29		22	45	31	51	39	51

14	53	32	31	47	37	59	27	45		38	12	58	41	45		12	38	48	31

ডিকোড করা বার্তা:

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

চেকপয়েন্ট 10: মৌলিক VPN FAQ (অংশ A)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ব্যবহার সম্পর্কে সম্ভাব্য গ্রাহকদের সবচেয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: VPN কী এবং এটি কীভাবে কাজ করে?

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) আপনার ইন্টারনেট সংযোগ এনক্রিপ্ট করে এবং ট্রাফিককে একটি নিরাপদ রিমোট সার্ভারের মধ্য দিয়ে পাঠায়। এতে আপনার পাবলিক IP অ্যাড্রেস আড়াল হয় এবং VPN টানেল দিয়ে যাওয়া ট্রাফিক সম্পর্কে স্থানীয় নেটওয়ার্ক পর্যবেক্ষক ও আপনার ISP কী দেখতে পারে, তা সীমিত হয়।

Q2: আমি কেন VPN ব্যবহার করব?

VPN আপনার ডিজিটাল গোপনীয়তা সুরক্ষা করে, পাবলিক Wi-Fi নেটওয়ার্কে (যেমন ক্যাফে বা বিমানবন্দরে) আপনার সংযোগ নিরাপদ রাখে, ISP এনক্রিপ্টেড ট্রাফিকের ধরন শনাক্ত করতে না পারলে কার্যকলাপভিত্তিক থ্রটলিং কমাতে পারে, ভৌগোলিক নিষেধাজ্ঞা এড়িয়ে বৈশ্বিক কনটেন্টে প্রবেশের সুযোগ দেয় এবং রিমোট কাজের রিসোর্স সুরক্ষিত রাখতে সহায়তা করে।

Q3: VPN কি আমাকে অনলাইনে সম্পূর্ণ বেনামি করে দেয়?

না। VPN আপনার IP ঠিকানা লুকায় ও ট্রাফিক এনক্রিপ্ট করলেও ব্রাউজার কুকি, সক্রিয় অ্যাকাউন্ট (যেমন Google বা Facebook), ব্রাউজার ফিঙ্গারপ্রিন্টিং, অথবা আপনার VPN প্রোভাইডার ডেটা লগ করলে আপনাকে তবুও ট্র্যাক করা যেতে পারে।

Q4: VPN কি আমার ইন্টারনেটের গতি কমিয়ে দেবে?

হ্যাঁ, সামান্য। এনক্রিপশন প্রক্রিয়া এবং VPN সার্ভারের ভৌত দূরত্ব ল্যাটেন্সি ও ওভারহেড যোগ করে। প্রভাব প্রদানকারী, প্রোটোকল, সার্ভারের দূরত্ব, ডিভাইস ও নেটওয়ার্ক অবস্থার ওপর নির্ভর করে বদলায়।

Q5: VPN ব্যবহার করা কি বৈধ?

অনেক দেশে VPN ব্যবহার বৈধ, তবে কিছু এখতিয়ারে VPN সেবা সীমিত, নিয়ন্ত্রিত বা ব্লক করা হয়। ব্যবহারের আগে ব্যবহারকারীদের বর্তমান স্থানীয় আইন যাচাই করা উচিত। আরও বিস্তারিত জানতে VPN.com-এর বৈধতা গাইড দেখুন।

চেকপয়েন্ট 10: মৌলিক VPN FAQ (অংশ B)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ব্যবহার সম্পর্কে সম্ভাব্য গ্রাহকদের সবচেয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: আমি কি ফ্রি VPN ব্যবহার করতে পারি?

ফ্রি VPN বিজ্ঞাপন, সীমিত ফিচার, ব্যবহার বিশ্লেষণ, ডেটা সীমা বা অন্যান্য আয়ের মডেলের ওপর নির্ভর করতে পারে। ব্যবহারের আগে প্রদানকারীর গোপনীয়তা নীতি, মালিকানা, অডিট ও ব্যবসায়িক মডেল দেখে নেওয়া উচিত।

Q7: "নো-লগস" নীতি কী?

নো-লগ নীতি বলে দেয় প্রদানকারী কোন কার্যকলাপ ও সংযোগ ডেটা সংরক্ষণ করে না বলে দাবি করে। সঠিক পরিধি ভিন্ন হয়, তাই পাঠকদের নীতি এবং স্বাধীন নিরীক্ষার ফলাফল পর্যালোচনা করা উচিত।

Q8: আমি কীভাবে সেরা VPN বেছে নেব?

অডিটেড no-logs নীতি, শক্তিশালী প্রোটোকল (WireGuard, OpenVPN), নিরাপদ সার্ভার অবস্থান, দ্রুত গতি, শুধু-RAM সার্ভার, কিল সুইচ ফিচার এবং গোয়েন্দা-তথ্য বিনিময় জোটের (যেমন 5/9/14 আইজ) বাইরের এখতিয়ার খুঁজুন।

Q9: আমি কি আমার ফোন ও স্মার্ট টিভিতে VPN ব্যবহার করতে পারি?

হ্যাঁ। আধুনিক VPN প্রদানকারীরা iOS, Android, macOS, Windows, Linux ও স্মার্ট টিভির জন্য ডেডিকেটেড অ্যাপ দেয়, পাশাপাশি আপনার হোম নেটওয়ার্কের সব ডিভাইস সুরক্ষিত করতে রাউটার সেটআপও দেয়।

Q10: কিল সুইচ কী?

কিল সুইচ এমন একটি নিরাপত্তা ফিচার, যা VPN সংযোগ বিচ্ছিন্ন হলে আপনার ডিভাইসকে স্বয়ংক্রিয়ভাবে ইন্টারনেট থেকে বিচ্ছিন্ন করে দেয়। এতে আপনার এনক্রিপশনবিহীন ডেটা বা প্রকৃত IP অ্যাড্রেস ফাঁস হওয়া ঠেকানো যায়।

চেকপয়েন্ট 10: উন্নত VPN FAQ (অংশ C)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ও নিরাপদ টানেলিং প্রোটোকলের প্রযুক্তিগত ও কাঠামোগত দিক অন্বেষণ করুন।

Q1: WireGuard, OpenVPN ও IKEv2-এর মধ্যে পার্থক্য কী?

WireGuard একটি আধুনিক, হালকা প্রোটোকল (মাত্র ~4,000 লাইন কোড), যা দ্রুত গতি ও দ্রুত সংযোগ সময় দেয়। OpenVPN একটি অত্যন্ত নিরাপদ, বহু পরীক্ষিত ওপেন-সোর্স প্রোটোকল। নেটওয়ার্ক বদলানোর সময় দ্রুত পুনঃসংযোগের সক্ষমতার কারণে IKEv2 মোবাইল ডিভাইসের জন্য চমৎকার। [4]

Q2: ডাবল VPN বা Multi-Hop রাউটিং কী?

মাল্টি-হপ আপনার ট্রাফিককে পরপর দুই বা ততোধিক VPN সার্ভারের মধ্য দিয়ে রুট করে। এটি দ্বিতীয় একটি এনক্রিপশন স্তর যোগ করে এবং একটি সার্ভার আপস হলে দ্বিতীয় হপ থেকে আপনার আসল IP ঠিকানা লুকিয়ে রাখতে সাহায্য করে।

Q3: WebRTC লিকিং কী এবং VPN কীভাবে তা প্রতিরোধ করে?

WebRTC একটি ব্রাউজার প্রোটোকল, যা VPN সক্রিয় থাকলেও আপনার আসল লোকাল ও পাবলিক IP অ্যাড্রেস প্রকাশ করে দিতে পারে। প্রিমিয়াম VPN তাদের ডেস্কটপ/মোবাইল অ্যাপ ও ব্রাউজার এক্সটেনশনে WebRTC অনুরোধ ব্লক বা স্পুফ করে।

Q4: RAM-only সার্ভার কী এবং কেন তা গুরুত্বপূর্ণ?

প্রচলিত সার্ভার হার্ড ড্রাইভে ডেটা লেখে, যা বাজেয়াপ্ত বা আপস করা যেতে পারে। শুধু-RAM (ডিস্কবিহীন) সার্ভার পুরোপুরি অস্থায়ী মেমরিতে (RAM) চলে। সার্ভার রিবুট বা বন্ধ করলে মেমরিতে থাকা ডেটা মুছে যায়।

Q5: অবফাসকেশন কীভাবে VPN ব্লক এড়িয়ে যায়?

অবফাসকেশন (বা "স্টিলথ VPN") VPN ট্রাফিককে সাধারণ HTTPS ট্রাফিকের (পোর্ট 443) মতো দেখায়। এটি সরকার বা স্কুল/অফিস নেটওয়ার্কের VPN ব্লক করতে ব্যবহৃত ডিপ প্যাকেট ইন্সপেকশন (DPI) পার হতে সাহায্য করতে পারে।

চেকপয়েন্ট 10: উন্নত VPN FAQ (অংশ D)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ও নিরাপদ টানেলিং প্রোটোকলের প্রযুক্তিগত ও কাঠামোগত দিক অন্বেষণ করুন।

Q6: স্প্লিট টানেলিং কী এবং কখন এটি ব্যবহার করা উচিত?

স্প্লিট টানেলিং আপনাকে বেছে নিতে দেয় কোন অ্যাপগুলো এনক্রিপ্টেড VPN টানেলের মধ্য দিয়ে যাবে এবং কোনগুলো সরাসরি ইন্টারনেটে সংযুক্ত হবে। সংবেদনশীল ব্যাংকিং অ্যাপ VPN-এর মধ্য দিয়ে পাঠাতে এবং VPN-এর যোগ করা লেটেন্সি এড়াতে স্থানীয় গেম সরাসরি সংযুক্ত রাখতে এটি ব্যবহার করুন।

Q7: ফরওয়ার্ড সিক্রেসি (পারফেক্ট ফরওয়ার্ড সিক্রেসি) কীভাবে কাজ করে?

PFS নিশ্চিত করে যে প্রতিটি সেশনের জন্য আলাদা, অস্থায়ী এনক্রিপশন কী তৈরি হয়। ভবিষ্যতে প্রাইভেট কী ফাঁস হলেও তা দিয়ে অতীত বা ভবিষ্যৎ সেশন ডিক্রিপ্ট করা যায় না, কারণ সেগুলো স্বাধীন কী ব্যবহার করেছিল।

Q8: 5/9/14 Eyes জোট কী এবং কেন তা আমার জানা দরকার?

এথতিয়ার একজন প্রদানকারীকে যে আইনি প্রক্রিয়ার মুখোমুখি হতে হতে পারে তা প্রভাবিত করতে পারে, কিন্তু বাস্তব গোপনীয়তার ঝুঁকি আরও নির্ভর করে প্রদানকারী কোন ডেটা সংরক্ষণ করে, তার প্রযুক্তিগত স্থাপত্য, মালিকানা, স্বচ্ছতা প্রতিবেদন এবং অডিটের ইতিহাসের ওপর।

Q9: DNS লিক সুরক্ষা কী?

DNS লিক সুরক্ষা আপনার ডিভাইসকে ওয়েবসাইট লুকআপ কোয়েরি (DNS কোয়েরি) আপনার ISP-র সার্ভারের বদলে VPN-এর প্রাইভেট, এনক্রিপ্টেড DNS সার্ভারের মাধ্যমে পাঠাতে বাধ্য করে। এতে আপনার ISP আপনি কোন সাইটে যান তা ট্র্যাক করতে পারে না।

Q10: VPN কি ISP-র ইন্টারনেট থ্রটলিং এড়াতে পারে?

কখনও কখনও। ISP নির্দিষ্ট শনাক্তযোগ্য কার্যকলাপ বেছে ধীর করলে VPN সাহায্য করতে পারে, কিন্তু এটি কনজেশন, ডেটা ক্যাপ, অ্যাকাউন্ট-স্তরের গতিসীমা বা খারাপ নেটওয়ার্ক মান কাটিয়ে উঠতে পারবে না।

অংশ 11: 10টি আকর্ষণীয় VPN তথ্য ও বাস্তব অন্তর্দৃষ্টি

VPN-এর ইতিহাস, বাজার ও প্রযুক্তি সম্পর্কে এই অত্যন্ত মূল্যবান বাস্তব তথ্য ও অন্তর্দৃষ্টিগুলো দেখে নিন।

1. প্রথম VPN প্রটোকল

PPTP (Point-to-Point Tunneling Protocol) রিমোট-অ্যাক্সেস VPN সমর্থনের জন্য Microsoft সহ একটি ভেন্ডর গ্রুপ তৈরি করেছিল এবং 1999 সালের জুলাইয়ে RFC 2637 হিসেবে প্রকাশিত হয়। [6]

2. বাজারমূল্য নির্ধারণ

দূরবর্তী কাজের প্রয়োজন বৃদ্ধি ও প্রতিষ্ঠানের নিরাপত্তা চাহিদার কারণে বৈশ্বিক VPN বাজার দ্রুত বেড়েছে।

3. WireGuard বিপ্লব

WireGuard-এর কোডবেস অত্যন্ত সুবিন্যস্ত ও দক্ষতার জন্য নকশা করা, ফলে প্রচলিত প্রোটোকলের চেয়ে নিরাপত্তা দুর্বলতার জন্য নিরীক্ষা করা সহজ। [4]

4. কঠোর নিরীক্ষা মান

শীর্ষ VPN সরবরাহকারীরা স্বাধীন কোড পর্যালোচনা করতে এবং কোনো ব্যবহারকারীর কার্যকলাপ লগ না করার বিষয়টি যাচাই করতে বাইরের অডিটর (যেমন Cure53 বা PwC) নিয়োগ করে।

5. 5-Eyes জোটের উৎস

Five Eyes জোটের উৎপত্তি 1946 সালের US ও UK-এর মধ্যকার UKUSA সিগন্যাল-ইন্টেলিজেন্স চুক্তি থেকে, পরে এতে Canada, Australia ও New Zealand যোগ দেয়।

6. ডিপ প্যাকেট ইন্সপেকশন

ডিপ প্যাকেট ইন্সপেকশন (DPI) শুধু হেডার নয়, প্যাকেটের বিষয়বস্তু ও ট্রাফিক প্যাটার্নও পরীক্ষা করে, এবং কিছু ফায়ারওয়াল প্রচলিত VPN প্রোটোকল শনাক্ত ও ব্লক করতে এটি ব্যবহার করে।

7. কর্পোরেট ব্যবহার

বিশ্বজুড়ে এন্টারপ্রাইজ কর্মীদের একটি বড় অংশ অভ্যন্তরীণ ডেটাবেসে লগইন করতে নিরাপদ VPN ব্যবহার করেন, ফলে এটি একটি প্রধান নিরাপত্তা মানদণ্ড।

8. বিকেন্দ্রীকৃত VPN

বিকেন্দ্রীভূত VPN (dVPN) ট্রাফিককে পিয়ার-চালিত নোডের নেটওয়ার্কে ছড়িয়ে দেয়, ফলে একক কেন্দ্রীভূত প্রোভাইডারের ওপর নির্ভরতা কমে।

9. টর বনাম VPN অজ্ঞাতপরিচয়

VPN একটিমাত্র প্রদানকারীর মধ্য দিয়ে ট্রাফিক টানেল করে, আর Tor (দ্য অনিয়ন রাউটার) তিনটি স্বেচ্ছাসেবী রিলের (গার্ড, মিডল ও এক্সিট) মধ্য দিয়ে ট্রাফিক পাঠায়, ফলে কোনো একটি রিলে দুই প্রান্তই জানতে পারে না।

10. ডেটা ফাঁসের খরচ

VPN-সহ জিরো-ট্রাস্ট নিরাপদ অ্যাকসেস মডেল ব্যবহার সংস্থাগুলোকে বুদ্ধিবৃত্তিক সম্পত্তি রক্ষা করতে এবং ডেটা ব্রিচের আর্থিক প্রভাব কমাতে সাহায্য করে।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

এই ওয়ার্কশিটে ব্যবহৃত উদ্ধৃত প্রকাশনা, ক্রিপ্টোগ্রাফিক স্পেসিফিকেশন ও অফিসিয়াল নথির মান।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

উত্তরমালা: VPN কী ওয়ার্কশিট

1 প্রাথমিক কাজ

প্রোটোকল

সঠিক উত্তর: B

শিক্ষণ নোট

VPN-এর মূল কাজ হলো একটি এনক্রিপ্টেড টানেল তৈরি করা, যা প্যাকেট পেলোড ডেটা সুরক্ষিত রাখে এবং ব্যবহারকারীর পাবলিক IP অ্যাড্রেস আড়াল করে। সূত্র: IETF Tunnel RFC।

2 নেটওয়ার্ক টানেলিং

ল্যাটেন্সি

সঠিক উত্তর: D

শিক্ষণ নোট

টানেলিং প্রোটোকল মূল ডেটা প্যাকেটকে বাইরের বাহক প্যাকেটের ভেতরে এনক্যাপসুলেট করে, যাতে পাবলিক নেটওয়ার্কে নিরাপদে পার হওয়া যায়। সূত্র: IETF Tunnel RFC।

3 প্রশ্ন 3

সঠিক উত্তর: B

শিক্ষণ নোট

VPN ট্রাফিক সুরক্ষায় কোন এনক্রিপশন স্ট্যান্ডার্ড ব্যাপকভাবে ব্যবহৃত হয়? → আধুনিক AES-256 স্ট্যান্ডার্ড

4 এনক্রিপ্টেড উপাদান

রাউটিং নিয়ন্ত্রণ

সঠিক উত্তর: C

শিক্ষণ নোট

VPN IP ডেটা প্যাকেটের সম্পূর্ণ পেলোড অংশ এনক্রিপ্ট করে, ফলে ট্রান্সমিশনের বিষয়বস্তু গোপন থাকে। সূত্র: IETF Tunnel RFC।

5 প্রশ্ন 5

সঠিক উত্তর: A

শিক্ষণ নোট

এনক্রিপশন একটি অ্যালগরিদম ও একটি কী ব্যবহার করে প্লেইনটেক্সটকে পড়ার অযোগ্য সাইফারটেক্সটে রূপান্তর করে।

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 আড়িপাতা ব্লক IP মাস্কিং **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

এনক্রিপ্টেড টানেল নিশ্চিত করে যে স্থানীয় Wi-Fi নেটওয়ার্কে ডেটা আটককারীদের কাছে প্যাকেট পেলোড অপাঠ্য থাকে। তথ্যসূত্র: Deloitte Advisory।

7 হার্ডওয়্যার পরিবর্তন গতি **সঠিক উত্তর: মিথ্যা**

শিক্ষণ নোট

VPN হলো সফটওয়্যার-ভিত্তিক নেটওয়ার্ক টানেল এবং এটি ভৌতভাবে আপনার গেটওয়ে রাউটারের হার্ডওয়্যার বদলায় না। সূত্র: Cure53 Audit।

8 টানেলিং প্যাকেট স্নিফিং ঝুঁকি **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

টানেলিং কাজ করে মূল নেটওয়ার্ক প্যাকেটকে সঞ্চালনের জন্য ট্রান্সপোর্ট হেডারের ভেতরে মুড়ে। সূত্র: IETF Tunnel RFC।

9 সিমেট্রিক কী ফায়ারওয়াল **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

সিমেট্রিক ক্রিপ্টোগ্রাফি নেটওয়ার্ক স্ট্রিম এনক্রিপ্ট ও ডিক্রিপ্ট উভয় কাজেই একটি শেয়ার্ড কী ব্যবহার করে। সূত্র: WireGuard Project।

10 পাওয়ার ইমিউনিটি নো-লগ **সঠিক উত্তর: মিথ্যা**

শিক্ষণ নোট

VPN কেবল সক্রিয় সংযোগ সংকেত এনক্রিপ্ট করে; স্থানীয় বিদ্যুৎ বিভ্রাটে সেবা বন্ধ হওয়া এটি ঠেকাতে পারে না। সূত্র: EDRi Retention Guidelines।

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. টানেলিং	E 2. প্রটোকল	G 3. ব্যান্ডউইথ	A 4. সার্ভার
C 5. জিওব্লক	D 6. ফায়ারওয়াল	F 7. প্রাইভেসি	B 8. ISP

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 টানেলিং	2 ব্যান্ডউইথ	3 জিও-ব্লক	4 প্রোটোকল
5 ফায়ারওয়াল	6 সার্ভার		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 B – গোপনীয়তা	2 E – এনক্রিপশন	3 F – নজরদারি	4 G – পরিচয়
5 H – ডিভাইস	6 A – সার্ভার	7 D – অনলাইন	8 C – আইএসপি

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা টানেলিং, প্রটোকল ও ব্যান্ডউইথ 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।

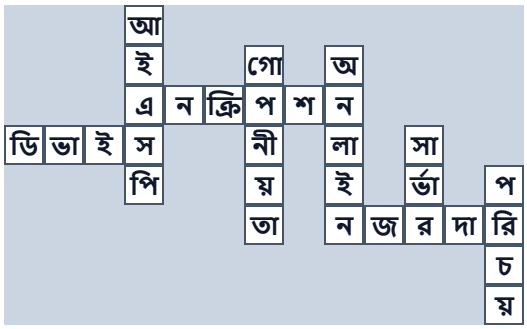
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ই	ট	লে	ছ	ণ	লে	তা	বি	নি	ঘ	ল	মি	কে	ভ	ড
রা	ন	র	ঈ	তি	গ	ই	সে	প	ভ	মা	ণ	জে	ঘ	চ
ই	ই	হ	ণ	দ	নে	স	ঝ	কা	রি	জ	রা	ফ	ঘ	উ
সে	লা	জি	আ	ড	প	পা	ধ	দ	জি	চ	কি	না	লি	ই
রে	ন	ফ	চ	ব	এ	দি	শ	জা	রা	দে	য়	ট	মে	র
ক	অ	সি	দ	ঠ	ন	হ	আ	সা	শ	মে	সা	র্ভা	র	দে
রা	কি	ঋ	তে	না	ক্রি	নে	ছ	ই	ষ	প	উ	অ	উ	ঋ
রি	মা	বা	য	ফ	প	বা	ম	দে	এ	তি	ভ	ঘ	রে	ষ
দা	ফ	ঘ	দ	হ	শ	স	ভ	রি	মি	স	ঢ	ষ	ষ	রি
র	সি	না	তি	তা	ন	ড	ঊ	নি	রা	কি	পি	থ	সে	ঊ
জ	গো	প	নী	য়	তা	লি	গ	নি	জা	পি	ঋ	জি	লি	ডি
ন	ট	ভ	ণ	জে	গ	স	ঘ	রে	দি	মি	ঋ	পা	ভা	উ
অ	জে	কা	গ	ম	আ	ঘ	কি	ঘ	ঝ	ণ	ধ	ই	গ	সি
রি	শ	ছ	দ	সে	জি	নি	ঝ	রে	পে	জ	স	আ	আ	রে
মা	স	মে	তি	দে	রি	ফ	সি	তি	সে	খ	স	বে	উ	ট

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

4 পাশাপাশি: এনক্রিপশন তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি (6 অক্ষর)

5 পাশাপাশি: ডিভাইস ফোন বা কম্পিউটারের মতো ব্যবহারযোগ্য যন্ত্র (4 অক্ষর)

8 পাশাপাশি: নজরদারি অনলাইন কার্যকলাপের ওপর গোপনে নজর রাখা (5 অক্ষর)

উপর-নিচ

1 উপর-নিচ: আইএসপি ইন্টারনেট সেবাদাতা, যারা এনক্রিপ্ট না করলে আপনার ট্র্যাফিক লগ করে (5 অক্ষর)

2 উপর-নিচ: গোপনীয়তা ট্র্যাকিং বা জনসাধারণের নজরদারি থেকে মুক্ত থাকার অবস্থা (5 অক্ষর)

3 উপর-নিচ: অনলাইন ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5 অক্ষর)

6 উপর-নিচ: সার্ভার আপনার ট্র্যাফিক রাউট করে ও আইপি আড়াল করা দূরবর্তী কম্পিউটার (3 অক্ষর)

7 উপর-নিচ: পরিচয় ব্যবহারকারীকে শনাক্তকারী তথ্য (4 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

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

শব্দ সাজানোর উত্তরমালা

1. ভ্রাসা — সার্ভার
2. আপিসএই — আইএসপি
3. এক্রিপনশন — এনক্রিপশন
4. য়চপরি — পরিচয়
5. নীতাগোয়প — গোপনীয়তা
6. ইঅলানন — অনলাইন
7. দারিনরজ — নজরদারি
8. ডিসইভা — ডিভাইস

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"নিরাপদ টানেলে গোপনীয়তা রক্ষা করুন"

কেস স্টাডির উত্তর

A পরিস্থিতি A: পাবলিক নেটওয়ার্ক নিরাপত্তা

স্নিফিং ও এনক্রিপশন | সারাহর উভয়সংকট

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- ঝুঁকি: প্যাকেট স্নিফিং, ডেটা ইন্টারসেপশন এবং ম্যান-ইন-দ্য-মিডল আক্রমণ। একই ক্যাফের নেটওয়ার্কে থাকা কেউ তার লগইনের তথ্য বা হোমওয়ার্ক ফাইল ধরে ফেলতে পারে।
- VPN সুরক্ষা: নেটওয়ার্ক প্যাকেটের পেলোড এনক্রিপ্ট করে, ফলে VPN সঠিকভাবে কনফিগার করা থাকলে আটকানো টানেল ট্রাফিক নিষ্ক্রিয় স্থানীয়-নেটওয়ার্ক আড়িপাতাকারীদের কাছে অপাঠ্য হয়ে যায়।

B পরিস্থিতি B: অবরুদ্ধ রিসোর্সে প্রবেশ

জিও-ব্লকিং ও IP | অ্যালেক্সের দ্বিধা

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- কেন ব্লক হয়েছে: স্ট্রিমিং হোস্ট জিও-ব্লকিং ব্যবহার করে, যা ভ্রমণকারী তার স্থানীয় IP অ্যাড্রেসকে তার ভৌত দেশের সঙ্গে মিলিয়ে ভৌগোলিক লাইসেন্সিংয়ের ভিত্তিতে ব্লক করে।
- VPN কীভাবে সাহায্য করে: নিজ দেশের সার্ভারের মাধ্যমে ট্রাফিক পাঠিয়ে তার আসল অবস্থান লুকানো। সাইটটি নিজ দেশের IP দেখে, ফলে অ্যাক্সেস পাওয়া যায়।