নাম: _____ তারিখ: _____ নম্বর: _____

পাবলিক Wi-Fi নিরাপত্তা ও এনক্রিপশন

ম্যান-ইন-দ্য-মিডল আক্রমণ, রগ অ্যাক্সেস পয়েন্ট, প্যাকেট স্নিফিং, VPN টানেল এবং HTTPS এনক্রিপশন।

পাবলিক Wi-Fi নিরাপত্তা 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 পাবলিক Wi-Fi নিরাপত্তা বিষয়ে গাইড করবে। আপনি এনক্রিপ্ট না করা নেটওয়ার্ক, ম্যান-ইন-দ্য-মিডল (MitM) আক্রমণ, রগ অ্যাক্সেস পয়েন্ট, প্যাকেট স্নিফিং, VPN টানেল এবং HTTPS ট্রানজিট নিরাপত্তা 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/public-wifi-suraksha/

আপনার পাবলিক Wi-Fi নিরাপত্তা শেখার রোডম্যাপ

- প্যাকেট স্নিফিং ও বেআইনি অ্যাক্সেস পয়েন্টসহ পাবলিক Wi-Fi-র সাধারণ ঝুঁকিগুলো শনাক্ত করুন।
- ট্রানজিট ডেটা সুরক্ষিত করতে VPN এনক্রিপশন টানেল বাস্তবায়ন করুন।
- রিমোট কর্মীদের জন্য HTTPS ও নিরাপদ ওয়েব ব্রাউজার সেটিংস কার্যকর করুন।

পাবলিক Wi-Fi নিরাপত্তা 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। রিমোট অ্যাক্সেস নিরাপত্তা বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

পাবলিক Wi-Fi নিরাপত্তা ও ট্রানজিট সুরক্ষা (ভূমিকা)

এনক্রিপ্ট-না-করা পাবলিক Wi-Fi হটস্পট নেটওয়ার্ক ট্রাফিককে প্যাকেট স্নিফিং ও Evil Twin স্পুফিংয়ের ঝুঁকিতে ফেলে। ট্রাফিককে সুরক্ষিত VPN এনক্রিপশন টানেলের মধ্য দিয়ে পাঠানো এবং শুধু-HTTPS HSTS নিয়ম প্রয়োগ করা সেশনকে স্থানীয় নেটওয়ার্কের আড়ি পাতা থেকে রক্ষা করে।

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

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. ম্যান-ইন-দ্য-মিডল (MitM) আক্রমণ কী?**

- A. শেয়ার্ড নেটওয়ার্কে দুই পক্ষের মধ্যকার যোগাযোগ আটকে পরিবর্তন করা
- B. ব্যবহারকারীর রেকর্ডকে লক্ষ্য করে ডেটাবেস নিষ্কাশনের কৌশল
- C. নেটওয়ার্ক ট্র্যাফিক অনুরোধে ওয়েব সার্ভারকে ভারাক্রান্ত করে ফেলা
- D. স্থানীয় হার্ড ড্রাইভের স্টোরেজ ভলিউম মুছে ফেলা

2 **2. রগ অ্যাক্সেস পয়েন্ট (ইভিল টুইন) কী?**

- A. বৈধ নেটওয়ার্কের একই SSID দিয়ে কনফিগার করা একটি ক্ষতিকর Wi-Fi হটস্পট
- B. ডেটাবেস ব্যাকআপ পর্যবেক্ষণে ব্যবহৃত প্রশাসনিক টুল
- C. একটি নিরাপদ VPN গেটওয়ে কনফিগারেশন
- D. অনুমোদিত মেইল সার্ভার ম্যাপ করা একটি DNS রেকর্ড

3 **3. VPN কীভাবে পাবলিক Wi-Fi ট্রাফিক সুরক্ষিত রাখে?**

- A. এটি সব নেটওয়ার্ক প্যাকেটকে এনক্রিপ্টেড টানেলে মুড়ে দেয়, ফলে স্নিফারদের কাছে তা অপাঠ্য হয়ে যায়
- B. এটি স্বয়ংক্রিয়ভাবে সব ইনকামিং সংযোগ অনুরোধ ব্লক করে
- C. এটি ফিজিক্যাল নেটওয়ার্ক কার্ডের MAC অ্যাড্রেস বদলে দেয়
- D. এটি ওয়েব ব্রাউজারে ক্যাশ করা কুকি মুছে ফেলে

4 **4. প্যাকেট স্নিফিং কী?**

- A. নেটওয়ার্ক প্যাকেট ধারণ ও লগ করতে হার্ডওয়্যার বা সফটওয়্যার টুল ব্যবহার করা
- B. ডুপ্লিকেট ফাইলের জন্য স্থানীয় ডিরেক্টরি স্ক্যান করা
- C. ব্যবহারকারীর ভূমিকা অনুযায়ী ডাটাবেস পড়ার অনুমতি সীমিত করা
- D. AES-256 কী ব্যবহার করে স্টোরেজ ড্রাইভ এনক্রিপ্ট করা

5 **5. HTTPS-এর ভূমিকা কী?**

- A. ব্রাউজার ও ওয়েব সার্ভারের মধ্যে সেশন ট্রাফিক এনক্রিপ্ট করা
- B. গেটওয়েতে ইনকামিং ইমেইল বার্তা ফিল্টার করা
- C. দ্রুত পৃষ্ঠা লোডের জন্য ছবি কমপ্রেস করা
- D. নেটওয়ার্ক-সংযুক্ত স্টোরেজে ফাইল কাঠামো পরিচালনা করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. সংযুক্ত ব্যবহারকারীরা উন্মুক্ত পাবলিক Wi-Fi নেটওয়ার্কে সহজেই প্লেইনটেক্সট ডেটা ধরে ফেলতে পারে।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. বেনামী অ্যাক্সেস পয়েন্ট (Evil Twin) সবসময় নেটওয়ার্ক অ্যাডমিনিস্ট্রেটরদের অনুমোদিত হয়।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. পাবলিক নেটওয়ার্কে প্যাকেট স্নিফিং থেকে ট্রাফিক সুরক্ষায় VPN অকার্যকর।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. HTTPS শুধু URL পাথ এনক্রিপ্ট করে, প্যাকেট পেলোড প্লেইনটেক্সটে রেখে দেয়।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. WPA3 নিরাপত্তা ব্যবহারকারী ওয়াই-ফাই হটস্পট খোলা, পাসওয়ার্ডহীন নেটওয়ার্কের চেয়ে বেশি সুরক্ষা দেয়।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

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

1. পাবলিক ওয়াই-ফাইয়ে ব্যক্তিগত পাসওয়ার্ড হাতিয়ে নেওয়া হলো যোগাযোগে _____ ।
2. স্থানীয় নেটওয়ার্কে কাঁচা প্যাকেট বিশ্লেষণে ব্যবহৃত হয় প্যাকেট _____ ।
3. হোটেলের ওয়াই-ফাইয়ের অনুকরণ করা ভুয়া হটস্পটকে বলা হয় _____ ।
4. ওয়েব ট্র্যাফিকের পরিবহন সুরক্ষিত করতে এনক্রিপ্ট করা দরকার _____ দিয়ে।
5. নেটওয়ার্কের সব আউটপুট এনক্রিপ্ট করতে ব্যবহৃত হয় ক্লায়েন্ট _____ ।
6. পাবলিক নেটওয়ার্কের মধ্য দিয়ে এনক্রিপ্টেড যোগাযোগ-পথ হলো একটি _____ ।

পরিভাষা শব্দভাণ্ডার

আড়িপাতা | ইভিল টুইন | টানেল | ডব্লিউপিএ থ্রি | ফায়ারওয়াল | ভিপিএন | স্নিফিং | HTTPS

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

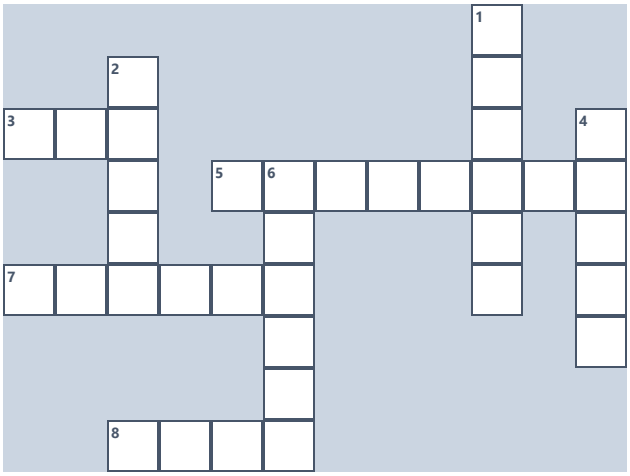
সংজ্ঞা মেলানো

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

☐	**1. আড়ি পাতা**	**A**	আধুনিক Wi-Fi নিরাপত্তা মান।
☐	**2. স্নিফিং**	**B**	ট্রানজিটে ডেটা চলার নিরাপদ পথ।
☐	**3. ইভিল টুইন**	**C**	ইনকামিং ট্রাফিক ফিল্টার করা।
☐	**4. HTTPS**	**D**	Wi-Fi-র নকল করা ভুয়া হটস্পট।
☐	**5. VPN**	**E**	ট্রানজিটে থাকা ট্রাফিক পড়া।
☐	**6. টানেল**	**F**	নেটওয়ার্ক ডেটা প্যাকেট ধরা।
☐	**7. WPA3**	**G**	এনক্রিপ্টেড ভার্চুয়াল প্রাইভেট নেটওয়ার্ক।
☐	**8. ফায়ারওয়াল**	**H**	নিরাপদ ওয়েব ট্রান্সমিশন।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

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



পাশাপাশি

3. ট্রানজিটে সুরক্ষিত ডেটা-পথ (3)

5. নিরাপদ ওয়েব সঞ্চালন (8)

7. আগত ট্র্যাফিক ছেঁকে দেখা (6)

8. এনক্রিপ্টেড ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (4)

উপর-নিচ

1. আধুনিক ওয়াই-ফাই নিরাপত্তা মান (6)

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

4. অ্যাকাউন্টে প্রবেশের গোপন সংকেত (5)

6. ওয়াই-ফাইয়ের অনুকরণ করা ভুয়া হটস্পট (6)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

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

পাশাপাশি

3 পাশাপাশি: ট্রানজিটে সুরক্ষিত ডেটা-পথ (3 অক্ষর):

5 পাশাপাশি: নিরাপদ ওয়েব সঞ্চালন (8 অক্ষর):

7 পাশাপাশি: আগত ট্র্যাফিক ছেঁকে দেখা (6 অক্ষর):

8 পাশাপাশি: এনক্রিপ্টেড ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (4 অক্ষর):

উপর-নিচ

1 উপর-নিচ: আধুনিক ওয়াই-ফাই নিরাপত্তা মান (6 অক্ষর):

2 উপর-নিচ: ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর):

4 উপর-নিচ: অ্যাকাউন্টে প্রবেশের গোপন সংকেত (5 অক্ষর):

6 উপর-নিচ: ওয়াই-ফাইয়ের অনুকরণ করা ভুয়া হটস্পট (6 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

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

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

পরিভাষা শব্দতালিকা

ইভিলটুইন, এইচটিটিপিএস, ভিপিএন, টানেল, ডব্লিউপিএথ্রি, ফায়ারওয়াল, ম্যালওয়্যার, পাসওয়ার্ড

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. ইভিলটুইন
B. এইচটিটিপিএস
C. ভিপিএন
D. টানেল
E. ডব্লিউপিএথ্রি
F. ফায়ারওয়াল
G. ম্যালওয়্যার
H. পাসওয়ার্ড

সংজ্ঞা ও মিলের ঘর
1. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার।
2. এনক্রিপ্টেড ভার্চুয়াল প্রাইভেট নেটওয়ার্ক।
3. নিরাপদ ওয়েব সঞ্চালন।
4. আগত ট্র্যাফিক ছেঁকে দেখা।
5. অ্যাকাউন্টে প্রবেশের গোপন সংকেত।
6. ওয়াই-ফাইয়ের অনুকরণ করা ভুয়া হটস্পট।
7. আধুনিক ওয়াই-ফাই নিরাপত্তা মান।
8. ট্রানজিটে সুরক্ষিত ডেটা-পথ।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

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

1. ল ই টু ই ন ভি
2. ভি এ ন পি
3. ড উ পি থ্রি এ ব্লি
4. ও র য়্যা ম্যা ল
5. টি পি ই স টি এ এ চ
6. নে ল টা
7. য়া ফা ও ল র য়া
8. র্ড পা ও য়া স

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

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

1	সফটওয়্যার আপডেট করার কারণ			
2	যেসব ডিভাইস স্বয়ংক্রিয়ভাবে Wi-Fi-তে সংযুক্ত হয়			
3	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
4	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
5	ক্যাফেতে নিরাপদ থাকার উপায়			
6	যেসব ডিভাইস হ্যাক হতে পারে			
7	খোলা Wi-Fi-তে একজন হ্যাকার যা যা দেখতে পারে			
8	ভুয়া Wi-Fi নেটওয়ার্কের লক্ষণ			
9	পাবলিক Wi-Fi-র বিকল্প			
10	ইমেইলে সতর্কতার লক্ষণ			
11	পাবলিক Wi-Fi-তে যা যা করা উচিত নয়			
12	ফ্রি Wi-Fi আছে এমন জায়গা			
13	আপনার অ্যাকাউন্ট সুরক্ষিত রাখার উপায়			
14	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
15	সন্দেহজনক মনে হয় এমন Wi-Fi নাম			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: পাবলিক Wi-Fi প্যাকেট স্নিফিং নিয়ন্ত্রণ



পরিস্থিতি: পাবলিক বিমানবন্দরের Wi-Fi নেটওয়ার্কে সংযুক্ত একজন রিমোট সেলস নির্বাহী লক্ষ্য করেন যে প্লেইনটেক্সটে পাঠানোর কিছুক্ষণ পরেই বেশ কয়েকটি সংবেদনশীল ব্যবসায়িক ইমেইল ফাঁস হয়ে গেছে।

আলোচনার প্রশ্ন: পাবলিক নেটওয়ার্কের ঝুঁকি বিশ্লেষণ করুন এবং একটি ট্রাফিক এনক্রিপশন সমাধানের রূপরেখা দিন।

কেস স্টাডি 2: ইভিল টুইন ভুয়া হটস্পট প্রতিরক্ষা



পরিস্থিতি: আক্রমণকারীরা একটি বৈধ ক্যাফে হটস্পটের নকল করে 'CoffeeShop_Guest' নামের একটি রগ ওয়্যারলেস অ্যাক্সেস পয়েন্ট স্থাপন করে এবং অসন্দিগ্ধ অতিথিদের নেটওয়ার্ক ট্রাফিক ধরে।

আলোচনার প্রশ্ন: রগ অ্যাক্সেস পয়েন্ট শনাক্ত ও ব্লক করার যাচাই ধাপগুলো বিস্তারিত বর্ণনা 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

35	46	32	46	8	31	51		32	45	34	39	46	12

10	37	59	45	3	33	45	3		42	48	38	12	58	41	46	27

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: পাবলিক Wi-Fi অনিরাপদ কেন?

খোলা পাবলিক Wi-Fi বাতাসে ট্রাফিক এনক্রিপ্ট করে না, তাই আশপাশের অন্যরা অরক্ষিত যেকোনো ডেটা ধরে ফেলতে পারে। [2]

Q2: প্যাকেট স্নিফিং কী?

প্যাকেট স্নিফার নেটওয়ার্ক ইন্টারফেস দিয়ে প্রবাহিত কাঁচা ডেটা ধারণ করে, ফলে প্লেইনটেক্সট পাসওয়ার্ড ও ট্রাফিকের বিবরণ প্রকাশ পেয়ে যায়।

Q3: Evil Twin কী?

হ্যাকারদের তৈরি একটি ভুয়া অ্যাক্সেস পয়েন্ট, যা বিশ্বস্ত স্থানীয় Wi-Fi হটস্পটের নাম ও সেটিংস নকল করে।

Q4: VPN কীভাবে আমাকে সুরক্ষা দেয়?

এটি আপনার ট্রাফিক এনক্রিপ্টেড টানেলের মাধ্যমে রাউট করে, ফলে স্থানীয় নেটওয়ার্ক স্নিফারদের কাছ থেকে আপনার ব্রাউজিং কার্যকলাপ লুকানো থাকে।

Q5: পাবলিক Wi-Fi-তে HTTPS কি আমাকে সুরক্ষা দেয়?

হ্যাঁ, এটি আপনার ব্রাউজার ও ওয়েবসাইটের মধ্যে আদান-প্রদান হওয়া ডেটা এনক্রিপ্ট করে, আর VPN সুরক্ষার আরেকটি স্তর যোগ করে।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: WPA3 কী?

আধুনিক Wi-Fi Protected Access স্ট্যান্ডার্ড, যা শক্তিশালী এনক্রিপশন ও অফলাইন ডিকশনারি আক্রমণ থেকে সুরক্ষা দেয়। [1]

Q7: পাবলিক Wi-Fi কি ম্যালওয়্যার পৌঁছে দিতে পারে?

হ্যাঁ, আক্রমণকারীরা ট্রাফিক আটকে আপনার ব্রাউজার সেশনে ক্ষতিকর ডাউনলোড প্রম্পট (ড্রাইভ-বাই ডাউনলোড) ঢুকিয়ে দিতে পারে।

Q8: ফাইল শেয়ারিংয়ের ঝুঁকি কী?

ফাইল শেয়ারিং চালু থাকলে পাবলিক নেটওয়ার্কের অন্য ব্যবহারকারীরা আপনার স্থানীয় ফোল্ডার ডিরেক্টরি পড়তে বা পরিবর্তন করতে পারে।

Q9: ক্যাপটিভ পোর্টাল কী?

হোটেল বা ক্যাফের নেটওয়ার্ক ইন্টারনেট অ্যাক্সেস দিতে যে লগইন পেজ ব্যবহার করে, যা কখনো কখনো আক্রমণকারীরা নকল করতে পারে।

Q10: ব্যবহার না করলে কি Wi-Fi বন্ধ রাখা উচিত?

হ্যাঁ, Wi-Fi বন্ধ রাখলে আপনার ডিভাইস অবিশ্বস্ত নেটওয়ার্কে স্বয়ংক্রিয়ভাবে সংযুক্ত হয় না।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

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

Q1: ম্যান-ইন-দ্য-মিডল আক্রমণ কীভাবে DNS-কে কাজে লাগায়?

টার্গেট ডোমেইনের বদলে ব্রাউজারকে সদৃশ ফিশিং ল্যান্ডিং পৃষ্ঠায় পাঠাতে একটি ভুয়া রাউটারে DNS স্পুফিং ব্যবহার করে।

Q2: সেশন হাইজ্যাকিং কী?

পাবলিক Wi-Fi-তে এনক্রিপশনবিহীন সেশন কুকি স্নিফ করে ক্রেডেনশিয়াল লগইন এড়াতে সেটি ইমপোর্ট করা আক্রমণকারী।

Q3: SSL স্ট্রিপিং কী?

একটি MitM আক্রমণ, যেখানে আক্রমণকারী ব্যবহারকারীর নিরাপদ HTTPS অনুরোধকে এনক্রিপশনবিহীন HTTP-তে নামিয়ে এনে লগইন তথ্য প্লেইনটেক্সটে হাতিয়ে নেয়।

Q4: HSTS কীভাবে SSL স্ট্রিপিংয়ের বিরুদ্ধে সুরক্ষা দেয়?

HTTP Strict Transport Security ব্রাউজারকে শুধু HTTPS-এর মাধ্যমে সংযুক্ত হতে বাধ্য করে এবং এনক্রিপ্ট না করা HTTP-তে ফিরে যাওয়া প্রত্যাখ্যান করে। [3]

Q5: স্প্লিট-টানেল VPN কী?

একটি কনফিগারেশন, যা কেবল কর্পোরেট ট্রাফিক VPN দিয়ে পাঠায় এবং পাবলিক ইন্টারনেট ডেটা সরাসরি পাঠায়, ফলে লিক পথ প্রকাশের ঝুঁকি থাকতে পারে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

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

Q6: WPA2 কেন KRACK-এর কাছে দুর্বল?

Key Reinstallation Attack WPA2-এর ফোর-ওয়ে হ্যান্ডশেকের দুর্বলতা কাজে লাগিয়ে Wi-Fi পাসওয়ার্ড ছাড়াই প্যাকেট ডিক্রিপ্ট করে।

Q7: ক্লায়েন্ট আইসোলেশন কী?

একটি রাউটার নিরাপত্তা সেটিং, যা সংযুক্ত Wi-Fi ডিভাইসগুলোকে সরাসরি পরস্পরের সঙ্গে যোগাযোগ করতে বাধা দেয় এবং স্থানীয় স্নিফিং ব্লক করে।

Q8: আক্রমণকারীরা কীভাবে ভুয়া DNS সার্ভার ব্যবহার করে?

এরা ক্লায়েন্টদের কাছে ভুয়া DNS সার্ভার বরাদ্দ করতে দুষ্ট রাউটার কনফিগার করে, যাতে সব ওয়েব লুকআপ আটকে পরিবর্তন করতে পারে।

Q9: VPN কি আমার লোকাল MAC অ্যাড্রেস লুকাতে পারে?

না। MAC ঠিকানা স্থানীয় লেয়ার-2 শনাক্তকারী; এর বদলে আপনার ডিভাইসের বিল্ট-ইন MAC র‍্যান্ডমাইজেশন (প্রাইভেট ঠিকানা) সেটিং ব্যবহার করুন।

Q10: ক্যাপটিভ পোর্টাল স্পুফিং আক্রমণ কী?

বিনামূল্যের Wi-Fi অ্যাক্সেসের ছদ্মবেশে ক্রেডেনশিয়াল চুরি করতে ভুয়া হটস্পটে জাল অথেন্টিকেশন পোর্টাল হোস্ট করা আক্রমণকারী।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

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

1. নিরাপত্তা ইনসাইট

রিমোট কর্মীরা প্রায়ই ক্যাফে, হোটেল ও বিমানবন্দরে Wi-Fi ব্যবহার করেন, যেখানে নেটওয়ার্কের নিরাপত্তা তাদের নিয়ন্ত্রণে থাকে না।

2. নিরাপত্তা ইনসাইট

ইভিল টুইন ভুয়া হটস্পট একটি বিশ্বস্ত নেটওয়ার্কের হুবহু নাম ও MAC অ্যাড্রেস নকল করে ডিভাইসকে বিভ্রান্ত করতে পারে।

3. নিরাপত্তা ইনসাইট

Wireshark-এর মতো প্যাকেট স্নিফিং সফটওয়্যার বিনামূল্যে পাওয়া যায় এবং এনক্রিপ্ট না করা HTTP পাসওয়ার্ড সাধারণ টেক্সটে দেখাতে পারে।

4. নিরাপত্তা ইনসাইট

WPA3 নিরাপত্তা স্থানীয় ব্রুট ফোর্স আক্রমণ থেকে রক্ষা করতে Simultaneous Authentication of Equals (SAE) ব্যবহার করে।

5. নিরাপত্তা ইনসাইট

SSL স্ট্রিপিং আক্রমণ গেটওয়েতে প্রাথমিক HTTP রিডাইরেক্ট ইন্টারসেপ্ট করে মৌলিক HTTPS সুরক্ষা এড়িয়ে যায়।

6. নিরাপত্তা ইনসাইট

HTTP Strict Transport Security (HSTS) রেসপন্স হেডার ব্রাউজারকে এনক্রিপ্ট না করা HTTP সংযোগে ফিরে যেতে বাধা দেয়। [3]

7. সিকিউরিটি ইনসাইট

'Auto-Connect' বন্ধ রাখলে স্মার্টফোন পাবলিক স্থানে একই রকম দেখতে দুষ্ট নেটওয়ার্কে সংযুক্ত হওয়া থেকে বিরত থাকে।

8. সিকিউরিটি ইনসাইট

এন্টারপ্রাইজ 'always-on' VPN কনফিগারেশন সব রিমোট কর্মীর নেটওয়ার্ক ট্রাফিক কর্পোরেট ফায়ারওয়ালের মধ্য দিয়ে যেতে বাধ্য করে।

9. সিকিউরিটি ইনসাইট

বেনামী অ্যাক্সেস পয়েন্ট জাল DNS উত্তর দিতে পারে, ফলে লক্ষ্য ডোমেইনগুলো ফিশিং সার্ভারে পুনঃনির্দেশিত হয়।

10. নিরাপত্তা ইনসাইট

VPN ছাড়া খোলা হটস্পটে অন্য ব্যবহারকারীরা দেখতে পারে আপনার ডিভাইস কোন সাইট ও সার্ভারের সঙ্গে যোগাযোগ করছে।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

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

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

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

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

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 — **সঠিক উত্তর: A**

শিক্ষণ নোট

ম্যান-ইন-দ্য-মিডল (MitM) আক্রমণ কী? → শেয়ার্ড নেটওয়ার্কে দুই পক্ষের মধ্যকার যোগাযোগ আটকে পরিবর্তন করা

2 প্রশ্ন 2 — **সঠিক উত্তর: A**

শিক্ষণ নোট

রগ অ্যাক্সেস পয়েন্ট (ইভিল টুইন) কী? → বৈধ নেটওয়ার্কের একই SSID দিয়ে কনফিগার করা একটি ক্ষতিকর Wi-Fi হটস্পট

3 প্রশ্ন 3 — **সঠিক উত্তর: A**

শিক্ষণ নোট

VPN কীভাবে পাবলিক Wi-Fi ট্রাফিক সুরক্ষিত রাখে? → এটি সব নেটওয়ার্ক প্যাকেটকে এনক্রিপ্টেড টানেলে মুড়ে দেয়, ফলে স্নিফারদের কাছে তা অপাঠ্য হয়ে যায়

4 প্রশ্ন 4 — **সঠিক উত্তর: A**

শিক্ষণ নোট

প্যাকেট স্নিফিং কী? → নেটওয়ার্ক প্যাকেট ধারণ ও লগ করতে হার্ডওয়্যার বা সফটওয়্যার টুল ব্যবহার করা

5 প্রশ্ন 5 — **সঠিক উত্তর: A**

শিক্ষণ নোট

HTTPS-এর ভূমিকা কী? → ব্রাউজার ও ওয়েব সার্ভারের মধ্যে সেশন ট্রাফিক এনক্রিপ্ট করা

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6

সঠিক উত্তর: সত্য

শিক্ষণ নোট

সংযুক্ত ব্যবহারকারীরা উন্মুক্ত পাবলিক Wi-Fi নেটওয়ার্কে সহজেই প্লেইনটেক্সট ডেটা ধরে ফেলতে পারে।

7 প্রশ্ন 7

সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: Evil Twin হলো আক্রমণকারীর তৈরি একটি অননুমোদিত হটস্পট, যা আসল হটস্পটের নকল করে।

8 প্রশ্ন 8

সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: VPN একটি টানেলে ট্রাফিক এনক্রিপ্ট করে, তাই লোকাল স্নিফাররা তা পড়তে পারে না।

9 প্রশ্ন 9

সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: HTTPS URL পাথ ও পেজের বিষয়বস্তুসহ পুরো HTTP আদান-প্রদান এনক্রিপ্ট করে।

10 প্রশ্ন 10

সঠিক উত্তর: সত্য

শিক্ষণ নোট

WPA3 নিরাপত্তা ব্যবহারকারী ওয়াই-ফাই হটস্পট খোলা, পাসওয়ার্ডহীন নেটওয়ার্কের চেয়ে বেশি সুরক্ষা দেয়।

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

E 1. আড়ি পাতা	F 2. স্নিফিং	D 3. ইভিল টুইন	H 4. HTTPS
G 5. VPN	B 6. টানেল	A 7. WPA3	C 8. ফায়ারওয়াল

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 আড়িপাতা	2 স্নিফিং	3 ইভিল টুইন	4 HTTPS
5 ভিপিএন	6 টানেল		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 G – ম্যালওয়্যার	2 C – ভিপিএন	3 B – এইচটিটিপিএস	4 F – ফায়ারওয়াল
5 H – পাসওয়ার্ড	6 A – ইভিলটুইন	7 E – ডব্লিউপিএথ্রি	8 D – টানেল

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা আড়ি পাতা, স্নিফিং ও ইভিল টুইন 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।

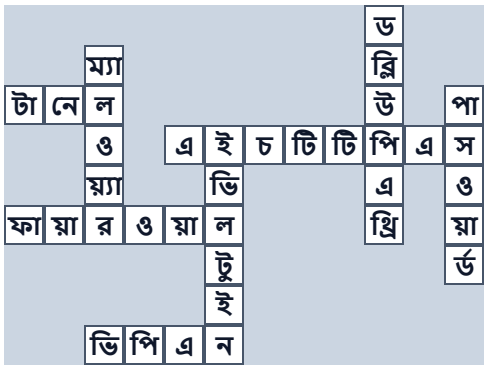
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

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

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

3 পাশাপাশি: টানেল ট্রানজিটে সুরক্ষিত ডেটা-পথ (3 অক্ষর)

5 পাশাপাশি: এইচটিটিপিএস নিরাপদ ওয়েব সঞ্চালন (8 অক্ষর)

7 পাশাপাশি: ফায়ারওয়াল আগত ট্র্যাফিক ছেঁকে দেখা (6 অক্ষর)

8 পাশাপাশি: ভিপিএন এনক্রিপ্টেড ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (4 অক্ষর)

উপর-নিচ

1 উপর-নিচ: ডব্লিউপিএথ্রি আধুনিক ওয়াই-ফাই নিরাপত্তা মান (6 অক্ষর)

2 উপর-নিচ: ম্যালওয়্যার ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর)

4 উপর-নিচ: পাসওয়ার্ড অ্যাকাউন্টে প্রবেশের গোপন সংকেত (5 অক্ষর)

6 উপর-নিচ: ইভিলটুইন ওয়াই-ফাইয়ের অনুকরণ করা ভুয়া হটস্পট (6 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

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

শব্দ সাজানোর উত্তরমালা

1. লইটুইনভি	**ইভিলটুইন**	5. টিপিইসটিএএচ	**এইচটিটিপিএস**
2. ভিএনপি	**ভিপিএন**	6. নেলটা	**টানেল**
3. ডউপিথ্রিএব্রি	**ডব্লিউপিএথ্রি**	7. য়াফাওলরয়া	**ফায়ারওয়াল**
4. ওরয়্যাম্যাল	**ম্যালওয়্যার**	8. র্ডপাওয়াস	**পাসওয়ার্ড**

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"ভিপিএনে পাবলিক ওয়াইফাই সুরক্ষিত"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: পাবলিক Wi-Fi প্যাকেট স্নিফিং নিয়ন্ত্রণ

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি পাবলিক বিমানবন্দর Wi-Fi নেটওয়ার্কে সংযুক্ত একজন রিমোট সেলস নির্বাহী লক্ষ্য করেন যে প্লেইনটেক্সটে পাঠানো বেশ কয়েকটি সংবেদনশীল ব্যবসায়িক ইমেল পাঠানোর অল্প পরেই ফাঁস হয়েছে।
- প্রস্তাবিত কৌশল ও সমাধান: সব রিমোট ওয়ার্কস্টেশনে এন্টারপ্রাইজ VPN ক্লায়েন্ট ব্যবহার বাধ্যতামূলক করুন। শুধু HTTPS ব্যবহারকারী ব্রাউজার এক্সটেনশন চালু করুন এবং ক্লায়েন্ট ফায়ারওয়ালে এনক্রিপ্ট না-করা প্রোটোকল (যেমন HTTP ও FTP) ব্লক করুন।

B কেস স্টাডি 2: ইভিল টুইন ভুয়া হটস্পট প্রতিরক্ষা

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: আক্রমণকারীরা একটি বৈধ ক্যাফে হটস্পটের অনুকরণে 'CoffeeShop_Guest' নামে একটি ভুয়া ওয়্যারলেস অ্যাক্সেস পয়েন্ট চালু করে এবং অসতর্ক অতিথিদের নেটওয়ার্ক ট্রাফিক ধরে ফেলে।
- প্রস্তাবিত কৌশল ও সমাধান: নেটওয়ার্কের সত্যতা যাচাই করতে অ্যাক্সেস পয়েন্টের BSSID MAC অ্যাড্রেস অডিট করুন। ওপেন নেটওয়ার্কে সংযোগ ব্লক করতে ক্লায়েন্ট পোসচার যাচাই কার্যকর করুন এবং সংবেদনশীল কাজের জন্য সেলুলার হটস্পট বাধ্যতামূলক করুন।