نام: _____ تاریخ: _____ نمره: _____

چگونه آدرس IP خود را پنهان کنیم کاربرگ

پنهان کردن آدرس‌های IP، پنهان‌سازی مکان، پروکسی، Tor و جلوگیری از نشت DNS/WebRTC

مرور یادگیری VPN

یادگیرنده
وضعیت دانشجویی
مسیر مدافع شبکه

امن
وضعیت اتصال
محافظت از بسته‌های داده

فعال
محافظت در برابر نشت
محافظت در برابر نشت DNS و IPv6

خوش آمدید! این بستهٔ فعالیت شما را در آشنایی با اصول بنیادین شبکه‌های خصوصی مجازی (VPN) راهنمایی می‌کند. می‌آموزید تونل‌های رمزگذاری‌شده چگونه از داده‌های شما محافظت می‌کنند، پروتکل‌های شبکه چگونه کار می‌کنند و چگونه می‌توان نشت‌های حریم خصوصی را شناسایی و کاهش داد.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: بر مفاهیم و پروتکل‌های VPN مسلط شوید.**
- ☐ **بخش 5-7: جدول‌های متقاطع و جدول‌های جست‌وجوی کلمه را حل کنید.**
- ☐ **بخش 8-9: مطالعات موردی و چالش رمز را حل کنید.**
- ☐ **بخش 10: صفحه‌های پرسش‌های متداول مقدماتی و پیشرفته را مرور کنید.**
- ☐ **بخش 11: 10 واقعیت جالب دنیای واقعی را کاوش کنید.**
- ☐ **تکمیلی: چالش سریع فکر کن**

باز کردن راهنمای VPN در VPN.com

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

نقشهٔ راه یادگیری VPN شما

- توضیح دهید نشانی‌های IP چگونه کار می‌کنند و چگونه موقعیت را نشت می‌دهند.
- پراکسی‌ها، Tor و VPNها را برای پنهان کردن نشانی‌های شبکه مقایسه کنید.
- روش‌های تشخیص و جلوگیری از نشت DNS و WebRTC را شناسایی کنید.
- درک کنید وب‌سایت‌ها کاربران را از طریق IP عمومی‌شان چگونه ردیابی می‌کنند.
- مسیریابی چندجهشی و تونل‌های رمزگذاری‌شده را برای حفاظت IP ارزیابی کنید.

راهنمای کاربرگ حفاظت از IP

به پرسش‌های چندگزینه‌ای و درست/نادرست پاسخ دهید، جمله‌های جای‌خالی را با استفاده از بانک واژه‌ها کامل کنید، تعاریف را تطبیق دهید و جدول‌های کلمات متقاطع و جست‌وجوی کلمه را حل کنید. دانسته‌های خود را درباره پنهان کردن نشانی IP و جلوگیری از نشت به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

پنهان کردن IP شما (مقدمه)

IP شما مانند یک نشانی پستی دیجیتال است که موقعیت فیزیکی و عادت‌های شبکه‌ای شما را آشکار می‌کند. پنهان کردن IP نخستین خط دفاع در برابر ردیابی آنلاین، پروفایل‌سازی هدفمند و مسدودسازی مبتنی بر موقعیت جغرافیایی است. درک چگونگی پنهان کردن امن نشانی‌تان به حفاظت از حریم خصوصی شما در فضای آنلاین کمک می‌کند.

هر ایستگاه بررسی را با دقت بخوانید و پاسخ درست را انتخاب کنید یا بنویسید.

ایستگاه بررسی 1: چالش چندگزینه‌ای

1. نشانی IP عمومی یک دستگاه چه چیزی را به وب‌سایت‌هایی که بازدید می‌کنید نشان می‌دهد؟

- A. شمارهٔ کارت اعتباری کاربر
- B. مکان تقریبی شما و نام ISP شما
- C. فهرست کامل فایل‌های محلی
- D. تنظیمات زبان صفحه‌کلید

2. کدام روش IP شما را پنهان می‌کند و همهٔ ترافیک را در سطح سیستم رمزگذاری می‌کند؟

- A. یک پراکسی وب استاندارد
- B. پاک کردن کوکی‌های مرورگر
- C. شبکهٔ خصوصی مجازی (VPN)
- D. غیرفعال کردن دیوار آتش بومی خود

3. محدودیت مهم حریم خصوصی در استفاده از پراکسی وب رایگان چیست؟

- A. ترافیک داده را در شبکه‌های عمومی رمزگذاری نمی‌کند
- B. نصب یک سیستم‌عامل خارجی را لازم دارد
- C. در ایالات متحده کاملاً غیرقانونی است
- D. به اتصال خط تلفن اختصاصی نیاز دارد

4. شبکهٔ Tor چگونه گمنامی بالا را برای کاربران فراهم می‌کند؟

- A. با تسریع سرعت اتصال
- B. با مسیریابی ترافیک از سه رلهٔ داوطلبانه
- C. با ثبت نام شما در یک پایگاه داده جهانی
- D. با محدود کردن دسترسی فقط به نهادهای دولتی

5. نشت DNS چیست؟

- A. خطا در ارسال ایمیل به نشانی اشتباه
- B. زمانی که پرس‌وجوهای DNS تونل VPN را دور می‌زنند و به ISP می‌روند
- C. خرابی سخت‌افزاری در منبع تغذیهٔ مسیریاب محلی
- D. به‌روزرسانی درایور آداپتور شبکهٔ محلی

ایستگاه بررسی 2: چالش درست یا نادرست

پرسش 6

6. سرور پراکسی ترافیک پس‌زمینهٔ سیستم‌عامل را مانند VPN رمزگذاری می‌کند.

درست نادرست

پرسش 7

7. مسیریابی Tor بسیار امن است اما سرعت مرور شبکه را کاهش می‌دهد.

درست نادرست

پرسش 8

8. نشت‌های WebRTC می‌توانند IP واقعی شما را در طول نشست فعال VPN افشا کنند.

درست نادرست

پرسش 9

9. وقتی VPN روشن است و نشتی وجود ندارد، ISP شما نمی‌تواند ببیند از کدام وب‌سایت‌ها بازدید می‌کنید.

درست نادرست

پرسش 10

10. پنهان کردن آدرس IP شما از ردیابی از طریق اثر انگشت مرورگر جلوگیری می‌کند.

درست نادرست

ایستگاه بررسی 3: درج اصطلاح کلیدی

هر جملهٔ زیر را بخوانید و جای خالی را با واژهٔ درست از بانک واژگان پر کنید.

1. عبور از تونل امن که پرس‌وجوهای دامنهٔ شما را آشکار می‌کند، _____ نام دارد.
2. APIهای ارتباطی مبتنی بر مرورگر مانند _____ ممکن است ناخواسته نشانی IP اصلی شما را فاش کنند.
3. یک _____ وب ترافیک مرورگر را هدایت می‌کند اما محتوای بسته‌ها را رمزگذاری نمی‌کند.
4. رمزگذاری چندلایهٔ شبکهٔ _____ سطح بالایی از ناشناسی فراهم می‌کند.
5. _____ عمومی شما را شرکت مخابراتی تخصیص می‌دهد و منطقهٔ شما را آشکار می‌کند.
6. دور زدن مسدودسازی‌های منطقه‌ای رسانه از طریق _____ مکان حاصل می‌شود.

بانک واژگان

پروکسی | پنهان‌سازی | تونل | ردیابی | نشانی IP | نشت DNS | Tor | WebRTC

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم شبکه

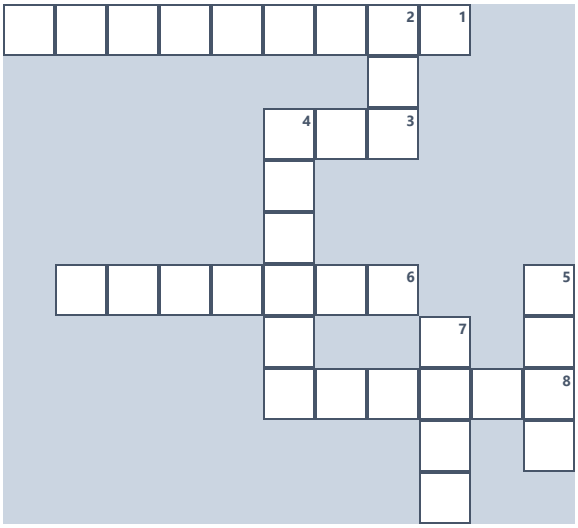
تطبیق تعاریف

هر اصطلاح واژگان در سمت راست را با نوشتن حرف متناظر (A-H) در کادر ورودی قابل‌پرکردن به تعریف درست آن در سمت چپ وصل کنید.

1. نشانی IP	A	تمام ترافیک یک دستگاه را رمزگذاری می‌کند و از طریق یک سرور VPN مسیریابی می‌کند.
2. تونل VPN	B	داده‌ها را از طریق سه سرور داوطلب هدایت می‌کند و در هر گام لایه‌ها را رمزگذاری می‌کند.
3. شبکهٔ Tor	C	مسیریابی اتصال از طریق سرور کشوری دیگر برای دور زدن مسدودسازی‌های جغرافیایی.
4. پراکسی وب	D	برچسب عددی یکتایی که رابط یک دستگاه را روی اینترنت مشخص می‌کند.
5. نشت DNS	E	ترافیک مرورگر را در لایهٔ برنامه و بدون رمزگذاری سیستمی هدایت می‌کند.
6. WebRTC API	F	ثبت مقصدهای ترافیک اینترنت رمزگذاری‌نشدهٔ شما توسط شرکت مخابراتی.
7. پنهان‌سازی موقعیت مکانی	G	پرس‌وجوهایی که خارج از تونل VPN تفکیک می‌شوند و دامنه‌های بازدیدشده را برای ISP آشکار می‌کنند.
8. ردیابی توسط ISP	H	قابلیت مرورگر برای صدا/تصویر که می‌تواند تونل‌ها را دور بزند و نشانی‌های IP واقعی را افشا کند.

ایستگاه بررسی 5: جدول‌کلمات

جدول کلمات متقاطع را با تایپ حروف در خانه‌های سفید فعال حل کنید. شماره‌ها با سرنخ‌های زیر مطابقت دارند.



افقی

1. هدایت اتصال از طریق سرور کشوری دیگر برای دور زدن محدودیت‌های جغرافیایی (9)

3. داده را از طریق سه سرور داوطلب مسیریابی می‌کند و در هر مرحله لایه‌ای را رمزگذاری می‌کند (3)

6. ویژگی مرورگر برای صدا و تصویر که می‌تواند تونل را دور بزند و نشانی IP واقعی را فاش کند (7)

8. ترافیک مرورگر را در لایهٔ برنامه بدون رمزگذاری سراسری سیستم هدایت می‌کند (6)

عمودی

2. پرس‌وجوهایی که بیرون از تونل VPN حل می‌شوند و دامنه‌های بازدیدشده را به ISP نشان می‌دهند (3)

4. ثبت مقصدهای ترافیک رمزگذاری‌نشدهٔ اینترنت توسط شرکت مخابراتی شما (6)

5. برچسب عددی یکتا که رابط یک دستگاه را در اینترنت شناسایی می‌کند (4)

7. تمام ترافیک دستگاه را رمزگذاری می‌کند و از طریق یک سرور VPN می‌فرستد (4)

ایستگاه بررسی 5 – فعالیت جایگزین: سرنخ‌های دسترس‌پذیر جدول‌کلمات

کاربران صفحه‌خوان و صفحه‌کلید می‌توانند پاسخ‌های جدول کلمات متقاطع را مستقیماً در فیلدهای متنی زیر تایپ کنند.

افقی

1 افقی: هدایت اتصال از طریق سرور کشوری دیگر برای دور زدن محدودیت‌های جغرافیایی (9 حرف):

3 افقی: داده را از طریق سه سرور داوطلب مسیریابی می‌کند و در هر مرحله لایه‌ای را رمزگذاری می‌کند (3 حرف):

6 افقی: ویژگی مرورگر برای صدا و تصویر که می‌تواند تونل را دور بزند و نشانی IP واقعی را فاش کند (7 حرف):

8 افقی: ترافیک مرورگر را در لایهٔ برنامه بدون رمزگذاری سراسری سیستم هدایت می‌کند (6 حرف):

عمودی

2 عمودی: پرس‌وجوهایی که بیرون از تونل VPN حل می‌شوند و دامنه‌های بازدیدشده را به ISP نشان می‌دهند (3 حرف):

4 عمودی: ثبت مقصدهای ترافیک رمزگذاری‌نشدهٔ اینترنت توسط شرکت مخابراتی شما (6 حرف):

5 عمودی: برچسب عددی یکتا که رابط یک دستگاه را در اینترنت شناسایی می‌کند (4 حرف):

7 عمودی: تمام ترافیک دستگاه را رمزگذاری می‌کند و از طریق یک سرور VPN می‌فرستد (4 حرف):

ایستگاه بررسی 6: جدول کلمات پنهان

8 اصطلاح کلیدی واژگان را که در جدول زیر پنهان شده‌اند پیدا کنید. کلمات می‌توانند افقی، عمودی یا مورب باشند.

ب	چ	ث	ی	خ	ط	ز	ف	ب	ث	ک	ب	س	ی	ظ
ف	پ	ث	ز	ظ	چ	ا	ض	چ	ص	ق	ذ	خ	س	ص
ع	ب	م	ف	ض	ی	ی	ذ	ذ	گ	ر	خ	ا	ک	ی
ر	و	ت	ظ	پ	ح	و	ظ	ه	ش	ن	ز	ج	و	ز
ض	ع	ن	ی	ظ	ش	غ	ص	ح	پ	ذ	غ	ت	ر	س
ل	ن	و	ت	پ	ر	ژ	ب	ج	ن	ق	ف	ک	پ	ت
ژ	و	ز	ژ	و	ط	ل	پ	ب	ه	ا	ن	ش	ت	ی
ژ	ص	ص	ذ	ث	ا	ر	ش	ع	ا	ث	ز	ک	ن	ب
پ	خ	ک	ک	د	ف	غ	ع	ش	ن	ش	خ	ظ	ع	ا
ت	گ	ه	ر	ق	ث	م	پ	ف	س	د	ض	ظ	ف	ی
ظ	ن	ن	ع	ث	ص	ث	ی	خ	ا	ز	ح	م	ی	د
ث	گ	ض	ث	ا	ژ	ث	ض	ی	ز	ا	ب	گ	پ	ر
ع	چ	ق	ی	ف	ذ	ج	ش	ع	ی	غ	ث	ذ	خ	چ
ف	ک	غ	ز	ع	و	ک	ظ	ص	ط	ع	ا	ا	چ	ل
ژ	ه	ه	ی	غ	ا	ر	م	ن	ف	ح	پ	ه	ص	ت

فهرست واژگان

ایپی
تونل
تور
پروکسی
نشت
بلادرنگ
پنهانسازی
ردیابی

ایستگاه بررسی 6 – فعالیت جایگزین: تطبیق دسترس‌پذیر واژگان

هر یک از 8 اصطلاح واژگان موجود در جدول کلمات پنهان را با نوشتن حرف (A-H) در جای خالی به تعریف درست آن وصل کنید.

اصطلاحات واژگان
A. اپپی
B. تونل
C. تور
D. پروکسی
E. نشت
F. بلادرنگ
G. پنهانسازی
H. ردیابی

	تعاریف و فیلدهای تطبیق
	1. ترافیک مرورگر را در لایهٔ برنامه بدون رمزگذاری سراسری سیستم هدایت می‌کند.
	2. هدایت اتصال از طریق سرور کشوری دیگر برای دور زدن محدودیت‌های جغرافیایی.
	3. ویژگی مرورگر برای صدا و تصویر که می‌تواند تونل را دور بزند و نشانی IP واقعی را فاش کند.
	4. برچسب عددی یکتا که رابط یک دستگاه را در اینترنت شناسایی می‌کند.
	5. داده را از طریق سه سرور داوطلب مسیریابی می‌کند و در هر مرحله لایه‌ای را رمزگذاری می‌کند.
	6. ثبت مقصدهای ترافیک رمزگذاری‌نشدهٔ اینترنت توسط شرکت مخابراتی شما.
	7. پرس‌وجوهایی که بیرون از تونل VPN حل می‌شوند و دامنه‌های بازدیدشده را به ISP نشان می‌دهند.
	8. تمام ترافیک دستگاه را رمزگذاری می‌کند و از طریق یک سرور VPN می‌فرستد.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی VPN آشکار شوند. پاسخ‌هایتان را در کادرهای پرشدنی بنویسید.

1. پ ا ی ی
2. ر و ت
3. ت ش ن
4. ن ی ز ا ا س پ ن ه
5. ل ت ن و
6. س ک پ و ی ر
7. ب ن ر گ ل د ا
8. ی ی ر ب ا د

فعالیت تکمیلی: سریع فکر کن

برای هر دسته 3 پاسخ بنویسید. هر کس زودتر فهرست را کامل کند برنده است.

1	دلایل استفاده از VPN در سفر		
2	مرورگرهایی که می‌شناسید		
3	چیزهایی که یک VPN می‌تواند پنهان کند		
4	واژه‌های مرتبط با حریم خصوصی		
5	واژه‌هایی از این کاربرگ که می‌خواهید به خاطر بسپارید		
6	چیزهایی که یک وب‌سایت می‌تواند از IP شما حدس بزند		
7	اعداد یا نمادهای موجود در یک نشانی IP		
8	افسانه‌ها دربارهٔ VPNها		
9	سرویس‌های VPN که می‌شناسید		
10	چیزهایی که ارائه‌دهندهٔ اینترنت شما می‌تواند ببیند		
11	وعده‌هایی که یک ارائه‌دهندهٔ VPN خوب می‌دهد		
12	چیزهایی که می‌توانند IP واقعی شما را نشت دهند		
13	دلایل پنهان کردن موقعیت مکانی		
14	روش‌های پنهان کردن نشانی IP		
15	دستگاه‌هایی که می‌توانند از VPN استفاده کنند		

ایستگاه بررسی 8: مطالعات موردی VPN

مفاهیمی را که آموخته‌اید برای حل سناریوهای واقعی زیر به کار ببرید.

سارا (دانشجوی کافه)

👩‍💻 «سلام! من در Coffee & Bytes نشسته‌ام. یک شبکهٔ عمومی ناامن به نام 'Free_Wi-Fi_No_Password' وجود دارد. می‌خواهم وارد ایمیل مدرسه‌ام شوم و تکلیفم را آپلود کنم، اما نگران هکرها هستم. استفاده از این شبکه بدون VPN چه خطرهایی دارد و VPN چگونه از داده‌های من محافظت می‌کند؟»

Alex (دانشجوی مسافر)

👨‍💻 «وای نه! برای یک پروژه به خارج از کشور سفر کرده‌ام و می‌خواهم یک مستند زیست‌شناسی را که روی سروری در کشور خودم میزبانی می‌شود تماشا کنم. اما سایت پیام 'This video is not available in your current location.' را نشان می‌دهد. چرا مسدود شده‌ام و VPN چگونه می‌تواند به تماشای آن کمک کند؟»

ایستگاه بررسی 9: رمزگشایی

برای تکمیل آموزش پنهان‌سازی IP، این پیام محرمانه دربارهٔ پنهان کردن ردپای دیجیتال خود را رمزگشایی کنید.

کلید رمزگذاری حرف به عدد

ا=1 ب=2 پ=3 ت=4 ث=5 ج=6 چ=7 ح=8 خ=9 د=10 ذ=11

ر=12 ز=13 ژ=14 س=15 ش=16 ص=17 ض=18 ط=19 ظ=20 ع=21 غ=22

ف=23 ق=24 ک=25 گ=26 ل=27 م=28 ن=29 و=30 ه=31 ی=32

29	1	31	29	3		1	12		10	30	9		32	29	1	16	29

10	32	29	25

پیام رمزگشایی‌شده:

نکته: هر عدد نشان‌دهندهٔ یک حرف فارسی از کلید بالا است.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش A)

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q1: VPN چیست و چگونه کار می‌کند؟

شبکهٔ خصوصی مجازی (VPN) اتصال اینترنت شما را رمزگذاری می‌کند و ترافیک شما را از طریق یک سرور راه‌دور امن عبور می‌دهد. این کار IP عمومی شما را پنهان می‌کند و آنچه ناظران شبکهٔ محلی و ISP شما دربارهٔ ترافیک عبوری از تونل VPN می‌بینند را محدود می‌کند.

Q2: چرا باید از VPN استفاده کنم؟

VPN از حریم خصوصی دیجیتال شما محافظت می‌کند، اتصال شما را در شبکه‌های Wi-Fi عمومی (مانند کافه‌ها یا فرودگاه‌ها) ایمن می‌کند، ممکن است وقتی ISP نوع ترافیک رمزگذاری‌شده را شناسایی نکند، کاهش سرعت مبتنی بر فعالیت را کم کند، محدودیت‌های جغرافیایی را دور می‌زند تا به محتوای جهانی دسترسی پیدا کنید، و به ایمن‌سازی منابع کار از راه دور کمک می‌کند.

Q3: آیا VPN مرا در فضای آنلاین کاملاً ناشناس می‌کند؟

خیر. هرچند VPN نشانی IP شما را پنهان و ترافیک را رمزگذاری می‌کند، همچنان می‌توانید از طریق کوکی‌های مرورگر، حساب‌های فعال (مانند Google یا Facebook)، انگشت‌نگاری مرورگر، یا اگر ارائه‌دهندهٔ VPN شما داده‌هایتان را ثبت کند، ردیابی شوید.

Q4: آیا پراکسی وب آدرس IP من را پنهان می‌کند؟

بله، اما فقط برای ترافیکی که از طریق آن ارسال می‌شود، معمولاً مرورگر شما. بیشتر پراکسی‌های وب داده‌های شما را رمزگذاری نمی‌کنند، بنابراین ISP یا اپراتور شبکه همچنان می‌تواند آنچه را ارسال و دریافت می‌کنید ببیند.

Q5: آیا پنهان کردن IP من قانونی است؟

در بسیاری از کشورها بله، اما برخی کشورها VPN و سایر ابزارهای پنهان کردن IP را محدود یا ممنوع می‌کنند. پنهان کردن IP هرگز یک عمل غیرقانونی را قانونی نمی‌کند، پس پیش از استفاده قوانین محلی را بررسی کنید.

ایستگاه بررسی 10: پرسش‌های متداول VPN – مقدماتی (بخش B)

رایج‌ترین پرسش‌ها و پاسخ‌هایی را که مشتریان بالقوه دربارهٔ استفاده از شبکه‌های خصوصی مجازی دارند مرور کنید.

Q6: آیا Tor آدرس IP من را پنهان می‌کند؟

بله. Tor ترافیک شما را از طریق سه رله داوطلب (محافظ، میانی و خروجی) می‌فرستد، بنابراین وب‌سایت‌ها نشانی رلهٔ خروجی را می‌بینند و هیچ رلهٔ منفردی هم نمی‌داند شما که هستید و به کجا می‌روید. [1]

Q7: IP من چه چیزی را آشکار می‌کند؟

IP عمومی شما معمولاً ISP و یک موقعیت تقریبی مانند کشور یا شهر شما را آشکار می‌کند. سایت‌ها همچنین می‌توانند از آن برای پیوند دادن بازدیدهای شما به یکدیگر و اعمال محدودیت‌های جغرافیایی استفاده کنند.

Q8: چگونه بررسی کنم که پنهان است؟

به VPN خود متصل شوید، سپس به یک سایت بررسی IP بروید و آزمون‌های نشت DNS و WebRTC را اجرا کنید. IP و سرورهای DNS نمایش‌داده‌شده باید متعلق به VPN باشند، نه ISP شما. اگر IP واقعی شما ظاهر شد، محافظت در برابر نشت را روشن کنید.

Q9: آیا می‌توانم VPN را روی گوشی و تلویزیون هوشمند خود استفاده کنم؟

بله. ارائه‌دهندگان مدرن VPN برنامه‌های اختصاصی برای Linux، Windows، macOS، Android، iOS و تلویزیون‌های هوشمند و همچنین راه‌اندازی روی روتر برای محافظت از همهٔ دستگاه‌های شبکهٔ خانگی شما ارائه می‌دهند.

Q10: کلید قطع (Kill Switch) چیست؟

Kill Switch قابلیتی امنیتی است که اگر اتصال VPN قطع شود، دستگاه شما را به‌طور خودکار از اینترنت جدا می‌کند. این کار از نشت داده‌های رمزگذاری‌نشده یا IP واقعی شما جلوگیری می‌کند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش C)

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q1: چرا پس از پنهان کردن نشانی IP هنوز وب‌سایت‌ها می‌توانند من را ردیابی کنند؟

پنهان کردن IP شما مانع اثر انگشت مرورگر نمی‌شود. ردیاب‌ها می‌توانند جزئیاتی مانند وضوح صفحه، فونت‌های نصب‌شده و تنظیمات مرورگر شما را در یک شناسه ترکیب کنند و کوکی‌ها یا حساب‌های واردشده نیز می‌توانند شما را شناسایی کنند، پس از یک مرورگر متمرکز بر حریم خصوصی هم استفاده کنید. [3]

Q2: مسیریابی دو VPN یا Multi-Hop چیست؟

روش چندجهشی ترافیک شما را به‌صورت متوالی از دو یا چند سرور VPN عبور می‌دهد. این کار لایهٔ رمزگذاری دوم اضافه می‌کند و اگر یک سرور آسیب ببیند، کمک می‌کند نشانی IP واقعی شما از جهش دوم پنهان بماند.

Q3: نشت WebRTC چیست و VPN چگونه از آن جلوگیری می‌کند؟

WebRTC یک پروتکل مرورگر است که حتی هنگام فعال بودن VPN می‌تواند نشانی‌های IP محلی و عمومی واقعی شما را فاش کند. VPNهای ممتاز درخواست‌های WebRTC را در برنامه‌های دسکتاپ/موبایل و افزونه‌های مرورگر خود مسدود یا جعل می‌کنند.

Q4: آیا ترافیک IPv6 می‌تواند آدرس IP واقعی من را فاش کند؟

بله، اگر VPN شما فقط IPv4 را تونل کند. در این صورت دستگاه شما ممکن است ترافیک IPv6 را خارج از تونل ارسال کند و نشانی اختصاص‌یافته از سوی ISP شما را افشا کند. از VPNی استفاده کنید که IPv6 را تونل یا مسدود می‌کند و آن را با آزمون نشت IPv6 تأیید کنید.

Q5: مبهم‌سازی چگونه مسدودسازی VPN را دور می‌زند؟

مبهم‌سازی (یا «Stealth VPN») بسته‌های ترافیک VPN را طوری پنهان می‌کند که شبیه ترافیک وب HTTPS معمولی (پورت 443) به نظر برسند. این کار به عبور از بازرسی عمیق بسته (DPI) کمک می‌کند که دولت‌ها یا شبکه‌های مدرسه و دفتر برای مسدود کردن VPN به کار می‌برند.

ایستگاه بررسی 10: پرسش‌های متداول VPN – پیشرفته (بخش D)

جنبه‌های فنی و ساختاری شبکه‌های خصوصی مجازی و پروتکل‌های تونل‌سازی امن را بررسی کنید.

Q6: آیا تونل‌بندی تفکیکی آدرس IP واقعی من را آشکار می‌کند؟

بله، برای برنامه‌هایی که مستثنا می‌کنید. ترافیکی که خارج از تونل ارسال می‌شود از IP واقعی شما استفاده می‌کند و RFC 8828 اشاره می‌کند که WebRTC می‌تواند نشانی ISP را در زیر یک VPN با تونل تقسیمی آشکار کند، مگر آنکه مرورگر آن را محدود کند. [2]

Q7: آدرس IP مشترک چیست و چگونه به حریم خصوصی کمک می‌کند؟

با IP مشترک، بسیاری از کاربران VPN هم‌زمان با یک نشانی یکسان آنلاین به نظر می‌رسند. این کار در مقایسه با IP اختصاصی که فقط شما از آن استفاده می‌کنید، مرتبط کردن یک بازدید واحد با شما را برای وب‌سایت بسیار دشوارتر می‌کند.

Q8: آیا ISP من می‌تواند ببیند که برای پنهان کردن IP از VPN استفاده می‌کنم؟

معمولاً بله. ISP شما می‌تواند ببیند به نشانی IP یک سرور VPN وصل می‌شوید، چه زمانی وصل می‌شوید و چه مقدار داده می‌فرستید، اما وب‌سایت‌هایی را که می‌بینید یا محتوای درون تونل رمزگذاری‌شده را نمی‌بیند.

Q9: محافظت در برابر نشت DNS چیست؟

محافظت در برابر نشت DNS دستگاه شما را وادار می‌کند پرس‌وجوهای جست‌وجوی وب‌سایت (پرس‌وجوهای DNS) را به‌جای سرورهای ISP شما، از طریق سرورهای DNS خصوصی و رمزگذاری‌شدهٔ VPN ارسال کند. این کار مانع می‌شود ISP شما بتواند ردیابی کند از چه سایت‌هایی بازدید می‌کنید.

Q10: برای پنهان کردن IP من پروکسی بهتر است یا VPN؟

VPN معمولاً بهتر است. IP شما را برای هر برنامهٔ دستگاه پنهان می‌کند و ترافیک را رمزگذاری می‌کند، در حالی که پراکسی وب معمولاً فقط مرورگر را پوشش می‌دهد و اغلب رمزگذاری اضافه نمی‌کند.

بخش 11: 10 واقعیت جالب و بینش‌های دنیای واقعی دربارهٔ VPN

این واقعیت‌ها و بینش‌های بسیار ارزشمند و دنیای واقعی دربارهٔ تاریخچه، بازار و فناوری VPNها را مرور کنید.

1. نخستین پروتکل VPN

PPTP (Point-to-Point Tunneling Protocol)، یک پروتکل VPN اولیه از گروهی به رهبری Microsoft در دههٔ 1990، اکنون ناامن به شمار می‌رود، بنابراین VPNهای مدرن از WireGuard یا OpenVPN استفاده می‌کنند.

2. اثرانگشت‌گیری

پنهان کردن IP شما مانع اثر انگشت مرورگر نمی‌شود، که می‌تواند شما را از روی جزئیاتی مانند وضوح صفحه و فونت‌های نصب‌شده شناسایی کند. [3]

3. انقلاب WIREGUARD

WireGuard کدبیس بسیار ساده‌شده‌ای دارد که برای کارایی طراحی شده و بررسی آسیب‌پذیری‌های امنیتی آن را از پروتکل‌های سنتی آسان‌تر می‌کند.

4. افشای نشانی WEBRTC

RFC 8828 هشدار می‌دهد که WebRTC می‌تواند هم آدرس عمومی VPN و هم آدرس ISP را که VPN روی آن اجرا می‌شود کشف کند، مگر اینکه مرورگر آن را محدود کند. [2]

5. خاستگاه اتحاد EYES-5

مشارکت اطلاعاتی Five Eyes شامل آمریکا، بریتانیا، کانادا، استرالیا و نیوزیلند از همکاری اطلاعات سیگنالی دوران جنگ جهانی دوم میان متفقین پدید آمد.

6. بازرسی عمیق بسته

دیوارهای آتش پیشرفته از بازرسی عمیق بسته (DPI) برای تحلیل فراداده‌های بستهٔ شبکه و مسدود کردن ویژگی‌های استاندارد اتصال VPN استفاده می‌کنند.

7. استفادهٔ مجدد از مدار TOR

Tor حدود ده دقیقه از یک مدار استفاده می‌کند و سپس مدار جدیدی می‌سازد، که پیوند دادن فعالیت مرور شما را دشوارتر می‌کند. [1]

8. VPNهای غیرمتمرکز

VPNهای غیرمتمرکز (dVPN) ترافیک را در شبکه‌ای از گره‌های مدیریت‌شده توسط همتایان توزیع می‌کنند و وابستگی به یک ارائه‌دهندهٔ متمرکز را کاهش می‌دهند.

9. گمنامی Tor در برابر VPN

VPN ترافیک را از یک ارائه‌دهندهٔ واحد عبور می‌دهد، در حالی که Tor (The Onion Router) ترافیک را از سه رله داوطلب (نگهبان، میانی، خروجی) می‌فرستد تا حریم خصوصی به بیشینه برسد. [1]

10. پراکسی‌ها در برابر تونل‌های VPN

پراکسی وب نشانی IPای را که سایت برای ترافیک مرورگر شما می‌بیند تغییر می‌دهد، اما برخلاف VPN معمولاً آن ترافیک را رمزگذاری نمی‌کند و برنامه‌های دیگر دستگاه شما را پوشش نمی‌دهد. [5]

منابع و مراجع فنی

نشریات ارجاع‌شده، مشخصات رمزنگاری و استانداردهای رسمی اسنادی که در سراسر این کاربرگ استفاده شده‌اند.

منابع علمی و صنعتی

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

کلید پاسخ: پنهان کردن نشانی‌های IP، پنهان‌سازی موقعیت مکانی، پروکسی، Tor و جلوگیری از نشت DNS/WebRTC

1 پرسش 1

پاسخ درست: B

نکتهٔ آموزشی

نشانی IP عمومی یک دستگاه چه چیزی را به وب‌سایت‌هایی که بازدید می‌کنید نشان می‌دهد؟ → مکان تقریبی شما و نام ISP شما

2 رمزگذاری سیستم VPN

تأخیر

پاسخ درست: C

نکتهٔ آموزشی

برخلاف پروکسی‌هایی که فقط ترافیک مرورگر را تغییر مسیر می‌دهند، VPN یک تونل رمزگذاری‌شدهٔ سراسر سیستم ایجاد می‌کند و برنامه‌های پس‌زمینه، بازی‌ها و پرس‌وجوهای سیستم‌عامل را ایمن می‌کند. منبع: Tor Project Relays, W3C WebRTC API.

3 نبود رمزگذاری در پروکسی

امنیت وای‌فای

پاسخ درست: A

نکتهٔ آموزشی

پراکسی‌های وب فقط ترافیک مرورگر را بدون رمزگذاری محتوای بسته‌ها هدایت می‌کنند؛ یعنی اپراتور شبکه یا ISP شما همچنان می‌تواند ترافیک محتوای شما را ردیابی کند. استناد: IETF Proxy Vulnerabilities.

4 پرسش 4

پاسخ درست: B

نکتهٔ آموزشی

شبکهٔ Tor چگونه گمنامی بالا را برای کاربران فراهم می‌کند؟ → با مسیریابی ترافیک از سه رلهٔ داوطلبانه

5 نشت‌های DNS تونل

حریم خصوصی

پاسخ درست: B

نکتهٔ آموزشی

نشت DNS زمانی رخ می‌دهد که درخواست‌های تفکیک نام دامنه از تونل VPN دور بزنند و مستقیم به حل‌کننده‌های ISP شما بروند و سوابق دامنه‌های بازدیدشده را افشا کنند. منبع: DNSSEC Tunnel Testing، EFF Tracking Evasion.

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **جزئیات محدودیت پروکسی** پنهان‌سازی IP

پاسخ درست: نادرست

نکتهٔ آموزشی

پروکسی‌ها در لایهٔ برنامه کار می‌کنند و یکپارچگی درایور شبکهٔ سراسری سیستم را که تونل VPN دارد، ندارند. منبع: IETF Proxy Vulnerabilities.

7 **پرسش 7**

پاسخ درست: درست

نکتهٔ آموزشی

عبور ترافیک از سه رلهٔ داوطلبانه با رمزگذاری لایه‌ای تأخیر اضافه می‌کند، بنابراین Tor معمولاً از اتصال مستقیم کندتر است.

8 **پرسش 8**

پاسخ درست: درست

نکتهٔ آموزشی

WebRTC می‌تواند نشانی‌های محلی و، در برخی تنظیمات VPN، IP عمومی اختصاص‌یافته توسط ISP را در زیر تونل آشکار کند (RFC 8828).

9 **پرسش 9**

پاسخ درست: درست

نکتهٔ آموزشی

بدون نشت DNS یا WebRTC، ISP فقط ترافیک رمزگذاری‌شده به سمت سرور VPN را می‌بیند، نه سایت‌هایی که بازدید می‌کنید.

10 **محدودیت‌های اثرانگشت‌گیری** بدون لاگ

پاسخ درست: نادرست

نکتهٔ آموزشی

اثرانگشت‌گیری معیارهای پیکربندی دستگاه (وضوح صفحه، قلم‌ها، افزونه‌ها) را هدف می‌گیرد که حتی وقتی IP پنهان است همچنان قابل‌مشاهده می‌مانند. منبع: EFF Tracking Evasion.

کلیدهای واژگان و معیار نمره‌دهی

بارم‌بندی معلم: برای هر تطبیق درست (در مجموع 8 امتیاز) و اصطلاح بافتی (در مجموع 6 امتیاز) 1 امتیاز بدهید.

ایستگاه بررسی 4: کلید پاسخ – تطبیق مفاهیم

D. 1. نشانی IP	A. 2. تونل VPN	B. 3. شبکهٔ Tor	E. 4. پراکسی وب
G. 5. نشت DNS	H. 6. WebRTC API	C. 7. پنهان‌سازی موقعیت مکانی	F. 8. ردیابی توسط ISP

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1. نشت DNS	2. WebRTC	3. پروکسی	4. Tor
5. نشانی IP	6. پنهان‌سازی		

ایستگاه بررسی 6 – فعالیت جایگزین: کلید پاسخ – تطبیق واژگان

1. D – پروکسی	2. G – پنهانسازی	3. F – بلادرنگ	4. A – اپی
5. C – تور	6. H – ردیابی	7. E – نشت	8. B – تونل

یادداشت‌های بحث برای مدرسان

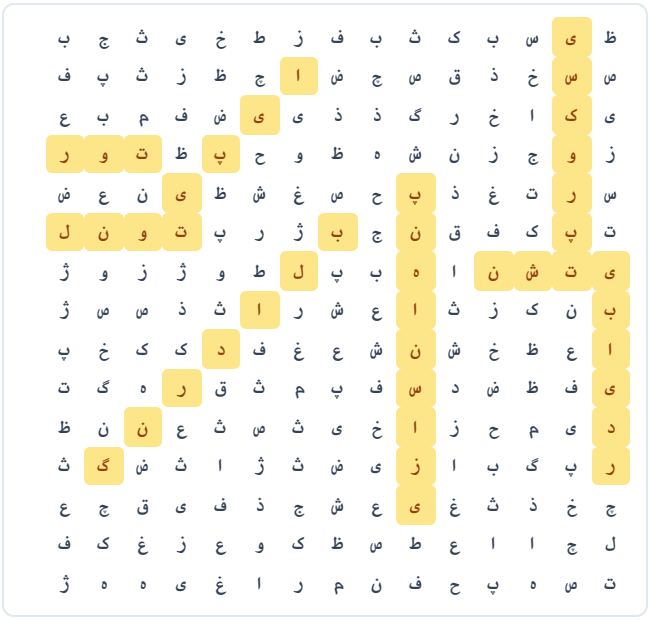
اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند نشانی IP، تونل VPN و شبکهٔ Tor را با کلمات خودشان توضیح دهند و برای هر کدام مثالی بزنند.

مطالعات موردی:
از دانش‌آموزان بخواهید پیشنهادهای خود را بر پایهٔ واقعیت‌های کاربرگ ارائه کنند، نه نظر شخصی.

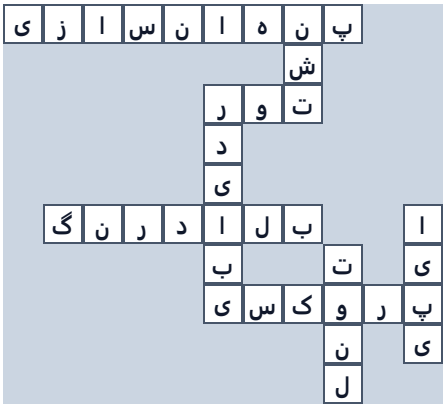
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات



پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

1 افقی: پنهانسازی هدایت اتصال از طریق سرور کشوری دیگر برای دور زدن محدودیت‌های جغرافیایی (9 حرف)

3 افقی: تور داده را از طریق سه سرور داوطلب مسیریابی می‌کند و در هر مرحله لایه‌ای را رمزگذاری می‌کند (3 حرف)

6 افقی: بلادرنگ ویژگی مرورگر برای صدا و تصویر که می‌تواند تونل را دور بزند و نشانی IP واقعی را فاش کند (7 حرف)

8 افقی: پروکسی ترافیک مرورگر را در لایهٔ برنامه بدون رمزگذاری سراسری سیستم هدایت می‌کند (6 حرف)

عمودی

2 عمودی: نشت پرس‌وجوهایی که بیرون از تونل VPN حل می‌شوند و دامنه‌های بازدیدشده را به ISP نشان می‌دهند (3 حرف)

4 عمودی: ردیابی ثبت مقصدهای ترافیک رمزگذاری‌نشدهٔ اینترنت توسط شرکت مخابراتی شما (6 حرف)

5 عمودی: اپی برچسب عددی یکتا که رابط یک دستگاه را در اینترنت شناسایی می‌کند (4 حرف)

7 عمودی: تونل تمام ترافیک دستگاه را رمزگذاری می‌کند و از طریق یک سرور VPN می‌فرستد (4 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. پایی — ایپی
2. روت — تور
3. تشن — نشت
4. نیزااسپنه — پنهانسازی
5. لتنو — تونل
6. سکپویر — پروکسی
7. بنرگلدا — بلادرنگ
8. ییرباد — ردیابی

کلید چالش رمز مخفی

"نشانی خود را پنهان کنید"

کلید پاسخ مطالعات موردی

A سناریو A: امنیت شبکهٔ عمومی

شنود و رمزگذاری — معمای سارا

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- خطرها: شنود بسته، رهگیری داده و حمله‌های مرد میانی. فردی در همان شبکهٔ کافه می‌تواند جزئیات ورود یا فایل تکلیف او را ضبط کند.
- محافظت VPN: محتوای بسته‌های شبکه را رمزگذاری می‌کند و وقتی VPN درست پیکربندی شده باشد، ترافیک تونل رهگیری‌شده را برای شنودگران منفعل شبکهٔ محلی ناخوانا می‌کند.

B سناریو B: دسترسی به منابع مسدودشده

مسدودسازی جغرافیایی و IPها — دوراهی Alex

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- دلیل مسدود شدن: میزبان پخش از مسدودسازی جغرافیایی استفاده می‌کند که IP محلی مسافر را به کشور فیزیکی او نگاشت می‌کند و بر اساس مجوزهای قلمرویی آن را مسدود می‌کند.
- VPN چگونه کمک می‌کند: پنهان کردن مکان واقعی او با مسیریابی ترافیک از طریق سروری در کشور خودش. سایت IP کشور خود او را می‌بیند و دسترسی را مجاز می‌کند.