نام: _____ تاریخ: _____ نمره: _____

محافظت از داده‌های شخصی و حقوق شما

داده‌های شخصی، حقوق حریم خصوصی (GDPR، CCPA)، دلالان داده، کوکی‌ها، فیشینگ، VPNها و حساب‌های ایمن‌تر

مرور آموزشی حریم خصوصی داده‌های شخصی

آگاهانه
داده‌های خود را بشناسید
چه چیزی جمع‌آوری می‌شود و چرا

توانمند
حقوق حریم خصوصی
حقوق GDPR و CCPA/CPRA

هوشیار
عادت‌های هوشمندانه
MFA، به‌روزرسانی‌ها و تشخیص کلاهبرداری

خوش آمدید! این بستهٔ فعالیت شما را در بررسی استانداردهای جهانی حریم خصوصی داده راهنمایی می‌کند. با رضایت صریح (opt-in) در GDPR، حق انصراف از فروش (opt-out) در CCPA، شیوه‌های کمینه‌سازی داده، رمزگذاری کامل دیسک در حالت ذخیره و TLS در حین انتقال آشنا می‌شوید.

ایستگاه‌های بررسی کاربرگ

- ☐ **بخش 1-4: با حقوق حریم خصوصی و عادت‌های ایمن خود آشنا 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 حریم خصوصی داده‌های VPN.com

URL: https://www.vpn.com/cybersecurity/data-privacy/

نقشهٔ راه یادگیری حریم خصوصی داده‌های شخصی شما

- حقوق حریم خصوصی خود را طبق GDPR و CCPA کالیفرنیا درک کنید.
- بشناسید که دلالان داده، کوکی‌ها و برنامه‌ها چگونه داده‌های شخصی را جمع‌آوری می‌کنند.
- با به اشتراک گذاشتن فقط آنچه یک سرویس واقعاً نیاز دارد، اصل کمینه‌سازی داده‌ها را به کار ببرید.
- در بنرهای کوکی و درخواست‌های مجوز برنامه، انتخاب‌های آگاهانه داشته باشید.
- با MFA و به‌روزرسانی‌ها، خطر ناشی از فیشینگ، نشت داده و Wi-Fi عمومی را کاهش دهید.

دستورالعمل‌های راهنمای حریم خصوصی داده

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 حفاظت از داده‌های شخصی خودتان به کار ببرید. و در پایان، فعالیت تکمیلی «سریع فکر کن».

حریم خصوصی داده‌های شخصی و حقوق شما (مقدمه)

حریم خصوصی داده یعنی توانایی شما برای کنترل نحوهٔ گردآوری، استفاده، ذخیره و اشتراک‌گذاری اطلاعات شخصی‌تان. قوانینی مانند GDPR و CCPA به شما حقوقی می‌دهند و عادت‌هایی مانند گذرواژه‌های قوی، MFA و اشتراک‌گذاری محتاطانه می‌توانند به کاهش خطر کمک کنند.

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

ایستگاه بررسی 1: چالش چندگزینه‌ای

1 1. کدام گزینه بهتر از همه اصل کمینه‌سازی داده را منعکس می‌کند؟

- A. اشتراک‌گذاری فقط داده‌ای که سرویس برای هدفش نیاز دارد
- B. دادن دسترسی کامل به هر برنامه برای ساده‌تر شدن راه‌اندازی
- C. پر کردن همهٔ فیلدهای اختیاری در فرم‌های ثبت‌نام
- D. استفادهٔ مجدد از یک گذرواژه تا مدیریت حساب‌ها آسان‌تر شود

2 2. اگر وب‌سایتی که استفاده می‌کنید نقض امنیتی گزارش کند، کدام گام توصیه می‌شود؟

- A. آن گذرواژه را تغییر دهید و در صورت امکان MFA را فعال کنید
- B. استفاده از همان گذرواژه برای یک حساب جدید
- C. با PIN خود به ایمیل نقض داده پاسخ دهید
- D. نادیده‌اش بگیرید، چون نقض داده‌ها به‌ندرت اهمیت دارند

3 3. طبق قواعد اتحادیهٔ اروپا، کدام مورد رضایت معتبر برای کوکی‌های ردیابی است؟

- A. علامت زدن فعالانهٔ یک کادر علامت‌نخورده پس از اطلاعات روشن
- B. کادرهای از پیش تیک‌خورده در بنر کوکی یا ثبت‌نام
- C. فقط ادامهٔ پیمایش یا مرور وب‌سایت
- D. اطلاعیه‌ای پنهان در شرایط و ضوابط سایت

4 4. مصرف‌کنندگان کالیفرنیایی بر اساس CCPA از کدام حق برخوردارند؟

- A. برای انصراف از فروش یا اشتراک‌گذاری داده‌های خود
- B. دریافت مبلغ ثابت به ازای هر درخواست داده
- C. برای درخواست حذف هر برنامه از فروشگاه‌های برنامه
- D. برای مسدود کردن همهٔ جمع‌آوری داده توسط همهٔ شرکت‌ها

5 5. وقتی به وای‌فای عمومی وصل می‌شوید، VPN عمدتاً چه کاری انجام می‌دهد؟

- A. ترافیک میان دستگاه شما و سرور VPN را رمزگذاری می‌کند
- B. مانع تنظیم هرگونه کوکی توسط وب‌سایت‌ها می‌شود
- C. جایگزین نیاز به MFA می‌شود
- D. بدافزار موجود روی دستگاه را حذف می‌کند

ایستگاه بررسی 2: چالش درست یا نادرست

6 پرسش درست/نادرست 6

6. حریم خصوصی داده و امنیت داده یک معنا دارند.

○ درست ○ نادرست

7 پرسش درست/نادرست 7

7. GDPR می‌تواند دربارهٔ شرکت‌های غیراروپایی که به افراد در اتحادیهٔ اروپا خدمات ارائه می‌دهند نیز اعمال شود.

○ درست ○ نادرست

8 پرسش درست/نادرست 8

8. استفاده از VPN مانع از ردیابی شما توسط وب‌سایت‌ها با کوکی‌ها می‌شود.

○ درست ○ نادرست

9 پرسش درست/نادرست 9

9. اشتراک‌گذاری کمتر داده‌های شخصی در اینترنت می‌تواند آسیب ناشی از نشت اطلاعات را کاهش دهد.

○ درست ○ نادرست

10 پرسش درست/نادرست 10

10. CCPA به مصرف‌کنندگان اجازه می‌دهد از فروش یا اشتراک‌گذاری داده‌هایشان انصراف دهند.

○ 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. طبق GDPR، _____ باید آزادانه، مشخص، آگاهانه و بدون ابهام داده شود، پس کادرهای از پیش تیک‌خورده پذیرفته نیستند.

2. یک _____ جزئیات را از سوابق عمومی، برنامه‌ها و خریدها گردآوری می‌کند تا نمایه‌هایی از افراد بسازد و بفروشد.

3. پیامکی که ادعا می‌کند بسته‌تان نگه داشته شده و از شما می‌خواهد مشخصات کارت را «تأیید» کنید، نمونهٔ معمول تلاش برای _____ است.

4. HTTPS از _____ استفاده می‌کند تا به محافظت از داده‌ها در مسیر میان مرورگر و وب‌سایت کمک کند.

5. ارائهٔ تنها جزئیاتی که فرم ثبت‌نام واقعاً نیاز دارد، اصل _____ را اعمال می‌کند.

6. حق _____ به شما اجازه می‌دهد از یک سازمان بخواهید داده‌های شخصی‌تان را حذف کند، هرچند استثناهایی وجود دارد.

بانک واژگان

انصراف | پاک‌سازی | دلال داده | رضایت | رمزگذاری | فیشینگ | کمینه‌سازی داده | کوکی

پاسخ‌های خود را اینجا بنویسید:

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

ایستگاه بررسی 4: تطبیق مفاهیم حریم خصوصی

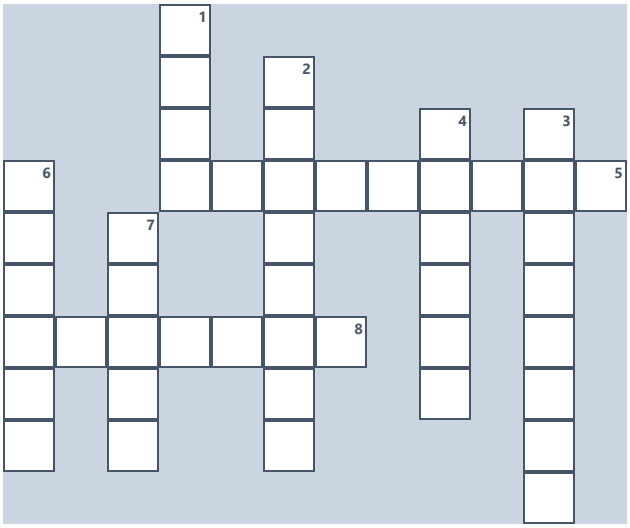
تطبیق تعاریف

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. حق پاک‌سازی	A	حق کالیفرنیایی‌ها برای متوقف کردن فروش یا اشتراک‌گذاری داده‌هایتان توسط یک کسب‌وکار.
2. حق انصراف	B	حق حذف داده‌های شخصی خود طبق GDPR، با رعایت استثناها.
3. کمینه‌سازی داده	C	فایل کوچک مرورگر که برای دنبال کردن فعالیت شما در وب‌سایت‌ها استفاده می‌شود.
4. رمزگذاری	D	توافق آزادانه، مشخص، آگاهانه و بدون ابهام.
5. کارگزار داده	E	جمع‌آوری فقط داده‌های شخصی لازم برای یک هدف اعلام‌شده.
6. رضایت	F	پیام‌های جعلی که مردم را فریب می‌دهند تا داده یا ورودهای خود را فاش کنند.
7. فیشینگ	G	درهم‌ریختن داده‌ها به‌گونه‌ای که فقط کسی که کلید درست را دارد بتواند آن‌ها را بخواند.
8. کوکی ردیاب	H	شرکتی که پروفایل‌های شخصی را از منابع متعدد جمع‌آوری و می‌فروشد.

ایستگاه بررسی 5: جدول‌کلمات

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



افقی

5. اصل گردآوری فقط آنچه برای هدف اعلام‌شده لازم است (9)

8. حقی که به شما اجازه می‌دهد از یک سازمان بخواهید داده‌های شخصی‌تان را حذف کند (7)

عمودی

1. فایل کوچک مرورگر که می‌تواند فعالیت شما را در وب‌سایت‌ها دنبال کند (4)

2. شرکتی که دربارهٔ افراد نمایه گردآوری می‌کند و می‌فروشد (8)

3. درهم‌ریختن داده تا فقط کسی که کلید درست دارد بتواند آن را بخواند (8)

4. حق CCPA برای توقف فروش یا اشتراک‌گذاری داده‌های شما (6)

6. پیام‌های جعلی که شما را فریب می‌دهند ورودها یا مشخصات کارت را فاش کنید (6)

7. موافقت آزادانه، مشخص، آگاهانه و بدون ابهام با استفاده از داده (5)

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

5 افقی: اصل گردآوری فقط آنچه برای هدف اعلام‌شده لازم است (9 حرف):

8 افقی: حقی که به شما اجازه می‌دهد از یک سازمان بخواهید داده‌های شخصی‌تان را حذف کند (7 حرف):

عمودی

1 عمودی: فایل کوچک مرورگر که می‌تواند فعالیت شما را در وب‌سایت‌ها دنبال کند (4 حرف):

2 عمودی: شرکتی که دربارهٔ افراد نمایه گردآوری می‌کند و می‌فروشد (8 حرف):

3 عمودی: درهم‌ریختن داده تا فقط کسی که کلید درست دارد بتواند آن را بخواند (8 حرف):

4 عمودی: حق CCPA برای توقف فروش یا اشتراک‌گذاری داده‌های شما (6 حرف):

6 عمودی: پیام‌های جعلی که شما را فریب می‌دهند ورودها یا مشخصات کارت را فاش کنید (6 حرف):

7 عمودی: موافقت آزادانه، مشخص، آگاهانه و بدون ابهام با استفاده از داده (5 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.

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

فهرست واژگان

پاکسازی انصراف کمینهسازی رمزگذاری دلالداده رضایت فیشینگ کوکی

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. پاکسازی
B. انصراف
C. کمینهسازی
D. رمزگذاری
E. دلالداده
F. رضایت
G. فیشینگ
H. کوکی

	تعاریف و فیلدهای تطبیق
	1. حق CCPA برای توقف فروش یا اشتراک‌گذاری داده‌های شما.
	2. موافقت آزادانه، مشخص، آگاهانه و بدون ابهام با استفاده از داده.
	3. شرکتی که دربارهٔ افراد نمایه گردآوری می‌کند و می‌فروشد.
	4. حقی که به شما اجازه می‌دهد از یک سازمان بخواهید داده‌های شخصی‌تان را حذف کند.
	5. اصل گردآوری فقط آنچه برای هدف اعلام‌شده لازم است.
	6. پیام‌های جعلی که شما را فریب می‌دهند ورودها یا مشخصات کارت را فاش کنید.
	7. فایل کوچک مرورگر که می‌تواند فعالیت شما را در وب‌سایت‌ها دنبال کند.
	8. درهم‌ریختن داده تا فقط کسی که کلید درست دارد بتواند آن را بخواند.

ایستگاه بررسی 7: چالش کلمات درهم‌ریخته

حروف زیر را مرتب کنید تا مفاهیم و اصطلاحات کلیدی امنیت سایبری آشکار شوند. پاسخ‌هایتان را در کادرهای ورودی ارائه‌شده بنویسید.

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

فعالیت تکمیلی: سریع فکر کن

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

1	گام‌هایی که پس از نقض داده باید برداشت		
2	برنامه‌هایی که موقعیت مکانی شما را می‌خواهند		
3	تنظیمات حریم خصوصی که روی یک گوشی جدید باید مرور کنید		
4	نشانه‌های آلوده بودن رایانه		
5	نشانه‌های اینکه یک پیام ممکن است فیشینگ باشد		
6	دلایل به‌روزرسانی نرم‌افزار		
7	جزئیات شخصی که باید از شبکه‌های اجتماعی دور بمانند		
8	روش‌های محافظت از حساب‌هایتان		
9	اطلاعاتی که هرگز نباید به اشتراک بگذارید		
10	حساب‌هایی که باید MFA روی آن‌ها روشن باشد		
11	چیزهایی که پشتیبان می‌گیرید		
12	جاهایی که ممکن است از Wi-Fi عمومی استفاده کنید		
13	کارهایی که پس از نشت داده باید انجام داد		
14	شرکت‌هایی که ممکن است داده‌های مرور شما را جمع کنند		
15	نشانه‌های هشدار در یک ایمیل		

ایستگاه بررسی 8: مطالعات موردی حریم خصوصی داده

مفاهیمی را که آموخته‌اید در سناریوهای واقعی زیر به کار ببرید.

مطالعهٔ موردی 1: درخواست از یک سایت برای حذف داده‌ها



سناریو: Maya که در فرانسه زندگی می‌کند، دو سال پیش حساب خود را در یک برنامهٔ خرید بست اما هنوز ایمیل‌های بازاریابی آن را دریافت می‌کند. او می‌خواهد برنامه داده‌های شخصی‌اش را طبق حق پاک‌شدن (right to erasure) در GDPR حذف کند.

پرسش برای بحث: Maya چه اقداماتی می‌تواند انجام دهد و برنامه چه داده‌هایی را ممکن است قانوناً نگه دارد؟

مطالعهٔ موردی 2: یک برنامهٔ آزمون و مجوزها



سناریو: یک برنامهٔ رایگان آزمون شخصیت پیش از شروع از Leo موقعیت مکانی، مخاطبان، میکروفون و تاریخ تولد او را می‌خواهد.

پرسش برای بحث: کدام مجوزها غیرضروری به نظر می‌رسند و Leo برای کاهش میزان اشتراک‌گذاری چه گزینه‌هایی دارد؟

ایستگاه بررسی 9: رمزگشایی

افراد آگاه به حریم خصوصی پیش از اشتراک‌گذاری جزئیات شخصی آنلاین مکث می‌کنند. از کلید حرف به عدد زیر برای رمزگشایی پیام استفاده کنید و حرف‌های متناظر را در جاهای خالی بنویسید.

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	32	1	27	29	1		25	1	12	4	16	1		13	1		16	32	3

10	32	29	25		12	25	23

پیام رمزگشایی‌شده:

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

ایستگاه بررسی 10: پرسش‌های متداول حریم خصوصی داده – مقدماتی (بخش A)

پرسش‌ها و پاسخ‌های رایج دربارهٔ حفاظت از داده‌های شخصی خود را مرور کنید.

Q1: تفاوت حریم خصوصی داده و امنیت داده چیست؟

حریم خصوصی کنترل شما بر نحوهٔ گردآوری، استفاده و اشتراک‌گذاری داده‌های شخصی است؛ امنیت حفاظتی است که آن‌ها را از دسترسی غیرمجاز نگه می‌دارد.

Q2: GDPR چیست؟

مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا (GDPR) که از 25 مه 2018 اجرا می‌شود، قواعد پردازش داده‌های شخصی را تعیین می‌کند و به افراد بر آن‌ها حقوقی می‌دهد [1].

Q3: CCPA چیست؟

قانون حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA)، با اصلاحیهٔ CPRA، به ساکنان حق دانستن، حذف، اصلاح و انصراف از فروش یا اشتراک‌گذاری داده‌ها را می‌دهد [4].

Q4: کمینه‌سازی داده به چه معناست؟

استفاده فقط از داده‌های شخصی که کافی، مرتبط و محدود به آنچه برای یک هدف لازم است باشند؛ به‌عنوان کاربر می‌توانید با کمتر به اشتراک گذاشتن آن را به کار ببندید [1].

Q5: مجوزهای برنامه چیستند؟

تنظیماتی که به برنامه‌ها اجازهٔ دسترسی به موقعیت مکانی، مخاطبان یا عکس‌های شما را می‌دهند؛ بازبینی آن‌ها و خاموش کردن موارد غیرضروری می‌تواند جمع‌آوری داده را محدود کند [8].

ایستگاه بررسی 10: پرسش‌های متداول حریم خصوصی داده – مقدماتی (بخش B)

پرسش‌ها و پاسخ‌های رایج دربارهٔ حفاظت از داده‌های شخصی خود را مرور کنید.

Q6: HTTPS برای حریم خصوصی من چه کاری انجام می‌دهد؟

HTTPS داده‌ها را بین مرورگر و سایت رمزگذاری می‌کند، اما سایت‌های کلاهبرداری هم می‌توانند از HTTPS استفاده کنند، پس قفل کنار آدرس ثابت نمی‌کند که سایت قابل اعتماد است [10].

Q7: حق پاک‌سازی (Right to Erasure) چیست؟

طبق ماده 17 GDPR می‌توانید در موارد معینی از یک سازمان بخواهید داده‌هایتان را حذف کند؛ این حق مطلق نیست و استثناهایی دارد [1].

Q8: چه چیزی رضایت معتبر محسوب می‌شود؟

اقدام تأییدی روشن، مانند علامت زدن کادر علامت‌نخورده پس از اطلاعات روشن؛ کادرهای از پیش علامت‌خورده، سکوت یا پیمایش صفحه به حساب نمی‌آیند [2].

Q9: چه چیزی گذرواژه را قوی می‌کند؟

طول مهم‌ترین است: NIST از سایت‌ها می‌خواهد برای گذرواژه‌هایی که به‌تنهایی استفاده می‌شوند حداقل 15 نویسه را الزامی کنند و استفاده از مدیر گذرواژه را مجاز بدانند [11].

Q10: پس از نشت داده باید چه کار کنم؟

گذرواژه‌های تحت تأثیر را تغییر دهید، MFA را فعال کنید، حساب‌هایتان را زیر نظر بگیرید و انجماد رایگان اعتبار را در نظر بگیرید؛ IdentityTheft.gov مراحل بازیابی را فهرست کرده است [9].

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

پرسش‌های عمیق‌تر دربارهٔ مبانی حقوقی، کوکی‌ها، ردیابی، دلالان داده و حقوق شما در فضای آنلاین را بررسی کنید.

Q1: آیا هر پردازش داده بر اساس GDPR به رضایت من نیاز دارد؟

خیر. رضایت یکی از شش مبنای قانونی در ماده 6 است؛ مبناهای دیگر شامل قرارداد، تکلیف قانونی و منافع مشروع هستند [1].

Q2: GDPR در کجا اعمال می‌شود؟

برای سازمان‌های مستقر در اتحادیهٔ اروپا و نیز سازمان‌های غیراروپایی که کالا یا خدمات به افراد در اتحادیهٔ اروپا ارائه می‌دهند یا رفتار آن‌ها را پایش می‌کنند [1].

Q3: آیا وب‌سایت‌ها برای همهٔ کوکی‌ها به رضایت نیاز دارند؟

همیشه نه. کوکی‌های کاملاً ضروری معمولاً معاف‌اند، اما کوکی‌های غیرضروری مانند کوکی‌های ردیابی به رضایت معتبر قبلی نیاز دارند [3].

Q4: خطر حریم خصوصی ردیاب‌های شخص ثالث چیست؟

ردیاب‌های شخص ثالث می‌توانند شما را در بسیاری از وب‌سایت‌ها دنبال کنند تا تبلیغات هدفمند نشان دهند؛ حذف کوکی‌ها و تنظیم گزینه‌های حریم خصوصی می‌تواند کمک کند [8].

Q5: دلال داده چیست؟

کسب‌وکاری که اطلاعات شخصی را از منابع مختلف جمع‌آوری می‌کند و به شرکت‌های دیگر می‌فروشد؛ ساکنان کالیفرنیا می‌توانند از پلتفرم DROP ایالت برای درخواست حذف استفاده کنند [5].

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

پرسش‌های عمیق‌تر دربارهٔ مبانی حقوقی، کوکی‌ها، ردیابی، دلالان داده و حقوق شما در فضای آنلاین را بررسی کنید.

Q6: پیوند CCPA با عنوان 'Do Not Sell or Share' چیست؟

کسب‌وکارهایی که داده می‌فروشند یا به اشتراک می‌گذارند عموماً باید پیوند 'Do Not Sell or Share My Personal Information' را ارائه کنند و به سیگنال‌های انصراف مانند GPC احترام بگذارند [4].

Q7: آیا VPN مرا ناشناس می‌کند؟

خیر. VPN ترافیک تا سرور VPN را رمزگذاری می‌کند و IP شما را از سایت‌ها پنهان می‌کند، اما ارائه‌دهنده آن را می‌بیند و کوکی‌ها و انگشت‌نگاری هنوز می‌توانند شما را ردیابی کنند [12].

Q8: چگونه یک پیام فیشینگ را تشخیص دهم؟

مراقب درخواست‌های فوری برای کلیک روی پیوندها، تأیید اطلاعات پرداخت یا رفع مشکلات حساب باشید؛ با شماره یا وب‌سایتی که مطمئنید واقعی است با شرکت تماس بگیرید [7].

Q9: آیا استفاده از Wi-Fi عمومی امن است؟

می‌تواند پرخطر باشد. بیشتر سایت‌ها از رمزگذاری استفاده می‌کنند، پس HTTPS را بررسی کنید، نرم‌افزار را به‌روز نگه دارید و از MFA استفاده کنید [10]؛ VPN می‌تواند در شبکه‌های نامطمئن حفاظت بیشتری اضافه کند [12].

Q10: حداکثر جریمه‌های مالی بر اساس GDPR چقدر است؟

برای جدی‌ترین تخلف‌ها، جریمه‌ها می‌تواند به 20 میلیون یورو یا 4% از گردش مالی سالانهٔ جهانی برسد، هر کدام که بیشتر باشد [1].

بخش 11: 10 واقعیت و بینش دنیای واقعی دربارهٔ حریم خصوصی داده

واقعیت‌های دنیای واقعی دربارهٔ قوانین حریم خصوصی، واسطه‌های داده، کلاهبرداری، نشت داده و عادت‌های امن‌تر آنلاین را مرور کنید.

1. بینش حریم خصوصی

GDPR از 25 مه 2018 اجرا می‌شود و به افراد حق دسترسی، اصلاح و پاک‌کردن داده‌های شخصی‌شان را می‌دهد [1].

2. بینش حریم خصوصی

طبق GDPR، جدی‌ترین نقض‌ها می‌توانند به جریمه تا 20 میلیون یورو یا 4% گردش مالی جهانی منجر شوند [1].

3. بینش حریم خصوصی

اصلاحیه‌های CPRA بر CCPA کالیفرنیا از 1 ژانویهٔ 2023 اجرایی شدند و حقوقی برای اصلاح داده‌ها و محدود کردن استفاده از داده‌های حساس افزودند [4].

4. بینش حریم خصوصی

به گزارش FTC، مصرف‌کنندگان اعلام کردند در سال 2025 مبلغ $15.9 billion بر اثر کلاهبرداری از دست داده‌اند، در حالی که سال قبل از آن بیش از $12 billion بود [6].

5. بینش حریم خصوصی

از 1 ژانویهٔ 2026، ساکنان کالیفرنیا می‌توانند از پلتفرم رایگان DROP استفاده کنند تا از دلالان داده بخواهند داده‌های شخصی آن‌ها را حذف کنند [5].

6. بینش حریم خصوصی

طبق قواعد حفاظت از داده اتحادیهٔ اروپا، کادرهای از پیش علامت‌خورده، سکوت یا بی‌عملی رضایت معتبر محسوب نمی‌شوند [2].

7. بینش حریم خصوصی

در بریتانیا، سایت‌ها باید راهی برای رضایت شما به هر کوکی که برای وب‌سایت کاملاً ضروری نیست فراهم کنند [3].

8. بینش حریم خصوصی

GDPR می‌گوید برخی نقض‌های داده‌های شخصی باید در صورت امکان ظرف 72 ساعت به مرجع مربوط گزارش شوند [1].

9. بینش حریم خصوصی

NIST می‌گوید سایت‌ها نباید تغییر دوره‌ای گذرواژه را تحمیل کنند و باید گذرواژه‌های جدید را با فهرست‌های افشاشده بررسی کنند [11].

10. بینش حریم خصوصی

VPN نشانی IP شما را از وب‌سایت‌ها پنهان می‌کند، اما ارائه‌دهندهٔ VPN همچنان می‌تواند ترافیک شما را ببیند، بنابراین با دقت انتخاب کنید [12].

منابع و مراجع فنی

راهنمای مطالعه و پازل‌ها از رهنمودهای رسمی حریم خصوصی اتحادیهٔ اروپا، بریتانیا، کالیفرنیا، NIST، FTC و EFF بهره می‌گیرند.

منابع رسمی و تخصصی

[1] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.
https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[3] Information Commissioner's Office. (n.d.). Cookies. ICO for the public.
https://ico.org.uk/for-the-public/online/cookies/

[4] California Privacy Protection Agency. (n.d.). Frequently asked questions (FAQs).
https://cppa.ca.gov/faq.html

[5] California Privacy Protection Agency. (2025). Delete Request and Opt-out Platform (DROP).
https://privacy.ca.gov/drop/

[6] Federal Trade Commission. (2026, March 25). FTC testifies before the Joint Economic Committee on agency's efforts to combat fraud [Press release].
https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud

[7] Federal Trade Commission. (2022). How to recognize and avoid phishing scams. Consumer Advice.
https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[8] Federal Trade Commission. (2023). How websites and apps collect and use your information. Consumer Advice.
https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information

[9] Federal Trade Commission. (2024). What to know about identity theft. Consumer Advice.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[10] Federal Trade Commission. (2023). Are public Wi-Fi networks safe? What you need to know. Consumer Advice.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[11] National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4).
https://csrc.nist.gov/pubs/sp/800/63/b/4/final

[12] Electronic Frontier Foundation. (2026). Choosing the VPN that's right for you. Surveillance Self-Defense.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

کلید پاسخ: ایستگاه بررسی 1 – چندگزینه‌ای

1 **کمینه‌سازی داده** کمینه‌سازی — پاسخ درست: **A**

نکتهٔ آموزشی

مادهٔ GDPR 5 الزام می‌کند داده‌های شخصی کافی، مرتبط و محدود به آنچه ضروری است باشند؛ کاربران می‌توانند با اشتراک‌گذاری کمتر از این اصل پیروی کنند [1].

2 **پاسخ به یک نقض امنیتی** نقض امنیتی — پاسخ درست: **A**

نکتهٔ آموزشی

پس از نقض داده، گذرواژه‌های افشاشده را تغییر دهید، MFA را فعال کنید و حساب‌ها را پایش کنید؛ IdentityTheft.gov مراحل بازیابی متناسب ارائه می‌دهد [9].

3 **رضایت معتبر** رضایت کوکی — پاسخ درست: **A**

نکتهٔ آموزشی

رضایت معتبر پس از اطلاعات روشن به یک اقدام تأییدی روشن نیاز دارد؛ کادرهای از پیش علامت‌خورده و ادامهٔ پیمایش واجد شرایط نیستند [2].

4 **حقوق CCPA** قانون CCPA — پاسخ درست: **A**

نکتهٔ آموزشی

مصرف‌کنندگان کالیفرنیایی می‌توانند از فروش یا اشتراک‌گذاری اطلاعات شخصی، از جمله از طریق سیگنال‌های Global Privacy Control، انصراف دهند [4].

5 **محافظت VPN** تونل VPN — پاسخ درست: **A**

نکتهٔ آموزشی

VPN ترافیک را تا سرور VPN رمزگذاری می‌کند و IP شما را از سایت‌ها پنهان می‌کند، اما کوکی‌ها و اثرانگشت مرورگر همچنان می‌توانند شما را ردیابی کنند [12].

کلید پاسخ: ایستگاه بررسی 2 – درست یا نادرست

6 **حریم خصوصی در برابر امنیت** حریم خصوصی
پاسخ درست: نادرست

نکتهٔ آموزشی

مرتبط اما متفاوت: ماده GDPR 5 قواعد استفاده از داده را تعیین می‌کند، در حالی که ماده 32 جداگانه اقدامات امنیتی را الزامی می‌داند [1].

7 **دامنهٔ شمول سرزمینی GDPR** دامنهٔ شمول GDPR
پاسخ درست: درست

نکتهٔ آموزشی

ماده 3(2) سازمان‌های خارج از اتحادیهٔ اروپا را که به افراد در اتحادیهٔ اروپا کالا یا خدمات ارائه می‌کنند یا رفتار آن‌ها را پایش می‌کنند، پوشش می‌دهد [1].

8 **VPN و کوکی‌ها** محدودیت‌های VPN
پاسخ درست: نادرست

نکتهٔ آموزشی

VPN نشانی IP شما را پنهان می‌کند، اما کوکی‌ها، پیکسل‌های ردیابی و اثرانگشت مرورگر همچنان می‌توانند شما را در وب‌سایت‌ها دنبال کنند [12].

9 **اشتراک‌گذاری کمتر** کمینه‌سازی
پاسخ درست: درست

نکتهٔ آموزشی

خاموش کردن مجوزهای غیرضروری برنامه‌ها و به‌اشتراک‌گذاری کمتر، آنچه را می‌توان جمع‌آوری کرد و بعداً در نقض داده فاش شود محدود می‌کند [8].

10 **انصراف از فروش یا اشتراک‌گذاری** قانون CCPA
پاسخ درست: درست

نکتهٔ آموزشی

کسب‌وکارهایی که داده می‌فروشند یا به اشتراک می‌گذارند باید پیوند انصراف روشنی مانند 'Do Not Sell or Share My Personal Information' ارائه کنند [4].

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

B 1. حق پاک‌سازی	A 2. حق انصراف	E 3. کمینه‌سازی داده	G 4. رمزگذاری
H 5. کارگزار داده	D 6. رضایت	F 7. فیشینگ	C 8. کوکی ردیاب

ایستگاه بررسی 3: کلید پاسخ – اصطلاحات کلیدی

1 رضایت	2 دلال داده	3 فیشینگ	4 رمزگذاری
5 کمینه‌سازی داده	6 پاک‌سازی		

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

1 B – انصراف	2 F – رضایت	3 E – دلالداده	4 A – پاکسازی
5 C – کمینهسازی	6 G – فیشینگ	7 H – کوکی	8 D – رمزگذاری

یادداشت‌های بحث برای مدرسان

اصطلاحات کلیدی:
بررسی کنید که دانش‌آموزان بتوانند حق پاک‌سازی، حق انصراف و کمینه‌سازی داده 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.

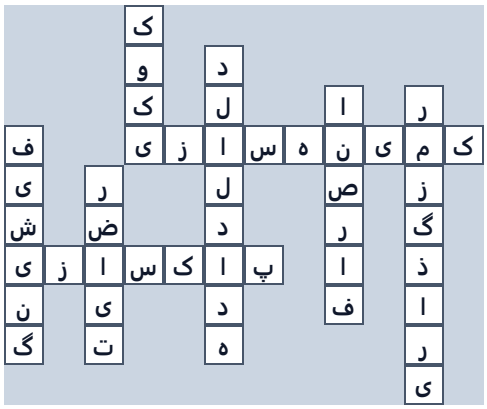
ارزیابی منابع:
از دانش‌آموزان بخواهید دست‌کم یک ادعا را در منابع کاربرگ بررسی کنند و دربارهٔ اینکه چرا ارقام، قیمت‌ها و قوانین ممکن است با گذشت زمان تغییر کنند گفت‌وگو کنید.

کلیدهای معما و یادداشت‌های معلم

پاسخ جدول کلمات

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

پاسخ جدول‌کلمات



راهنمای معلم برای پاسخ‌های جدول کلمات متقاطع

افقی

5 افقی: کمینه‌سازی اصل گردآوری فقط آنچه برای هدف اعلام‌شده لازم است (9 حرف)

8 افقی: پاکسازی حقی که به شما اجازه می‌دهد از یک سازمان بخواهید داده‌های شخصی‌تان را حذف کند (7 حرف)

عمودی

1 عمودی: کوکی فایل کوچک مرورگر که می‌تواند فعالیت شما را در وب‌سایت‌ها دنبال کند (4 حرف)

2 عمودی: دلالداده شرکتی که دربارهٔ افراد نمایه گردآوری می‌کند و می‌فروشد (8 حرف)

3 عمودی: رمزگذاری درهم‌ریختن داده تا فقط کسی که کلید درست دارد بتواند آن را بخواند (8 حرف)

4 عمودی: انصراف حق CCPA برای توقف فروش یا اشتراک‌گذاری داده‌های شما (6 حرف)

6 عمودی: فیشینگ پیام‌های جعلی که شما را فریب می‌دهند ورودها یا مشخصات کارت را فاش کنید (6 حرف)

7 عمودی: رضایت موافقت آزادانه، مشخص، آگاهانه و بدون ابهام با استفاده از داده (5 حرف)

کلید پاسخ کلمات درهم‌ریخته و رمزگشایی

کلید نمره‌دهی برای فعالیت بازچینی واژگان و چالش رمز مخفی.

کلید مرتب‌سازی کلمات

1. سزپایکا — پاکسازی
2. یکزنمساهی — کمینهسازی
3. للدداهدا — دلالداده
4. گیشنفی — فیشینگ
5. رصفاان — انصراف
6. ریگارذمز — رمزگذاری
7. یتراض — رضایت
8. کیکو — کوکی

کلید چالش رمز مخفی

"پیش از اشتراک آنلاین فکر کنید"

کلید پاسخ مطالعات موردی

A مطالعهٔ موردی 1: درخواست از یک سایت برای حذف داده‌ها

راهنمای معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: مایا که در فرانسه زندگی می‌کند، دو سال پیش حساب خود را در یک برنامهٔ خرید بست، اما هنوز ایمیل‌های بازاریابی آن را دریافت می‌کند. او می‌خواهد بر اساس حق پاک‌سازی در GDPR، برنامه داده‌های شخصی‌اش را حذف کند.
- رویکردهای توصیه‌شده: گزینهٔ 1: مایا درخواست کتبی پاک‌سازی ارسال می‌کند و به بازاریابی مستقیم اعتراض می‌کند که پس از آن باید متوقف شود؛ برنامه معمولاً باید ظرف یک ماه پاسخ دهد [1]. گزینهٔ 2: او ابتدا اشتراک را لغو می‌کند تا سریع آسوده شود. استدلال: پاک‌سازی مطلق نیست، بنابراین برنامه ممکن است داده‌های لازم برای تعهدات قانونی یا دعاوی حقوقی را نگه دارد [1]. اگر پاسخی ندهد، او می‌تواند به مرجع حفاظت از داده شکایت کند [1].

B مطالعهٔ موردی 2: یک برنامهٔ آزمون و مجوزها

راهنمای معلم

راهنمای نمره‌دهی

پاسخ‌های دانش‌آموز باید نکات زیر را پوشش دهد:

- تحلیل سناریو: یک برنامهٔ رایگان آزمون شخصیت پیش از شروع از لئو موقعیت مکانی، مخاطبین، میکروفون و تاریخ تولدش را می‌خواهد.
- رویکردهای توصیه‌شده: گزینهٔ 1: دسترسی به موقعیت مکانی، مخاطبان و میکروفون را رد کنید، سپس بررسی کنید که آیا آزمون همچنان کار می‌کند [8]. گزینهٔ 2: اگر برنامه اصرار کرد، برنامهٔ دیگری انتخاب کنید یا آن را حذف کنید [8]. استدلال: یک آزمون به ندرت به آن داده‌ها نیاز دارد و اشتراک‌گذاری کمتر، آنچه را می‌تواند جمع‌آوری، فروخته یا افشا شود محدود می‌کند. لئو همچنین می‌تواند مجوزها را به‌طور منظم در تنظیمات حریم خصوصی گوشی خود بررسی کند [8].