AVENQOR
EDUCATION ONLY

الأمان أولاً: الاحتيالات، التصيد، الحفظ

تدريب عملي لمكافحة الاحتيال

احمِ أصولك ومعرفتك.

احتيالات | تصيد | نظافة الحفظ

إشعار قانوني ومخاطر

- هذه الدورة لأغراض تعليمية فقط ولا تقدم نصيحة مالية.
- يمكن أن يؤدي التداول في الأسواق عالية المخاطر إلى خسائر مالية كبيرة.
- لا توجد ضمانات للربح في هذه الدورة.
- تحقق دائمًا من المعلومات بشكل مستقل قبل التصرف.
- لا تؤيد هذه الدورة أي منصة تداول أو منتج معين.

هذا ليس مناسباً لـ

- الأفراد الذين يبحثون عن أرباح مضمونة.
- أولئك الذين لا يرغبون في قبول المخاطر المرتبطة بالتداول.
- الأشخاص الذين يبحثون عن نصائح استثمارية محددة.

كيفية استخدام هذه الدورة

الوتيرة الموصى بها

- خذ وقتك لفهم كل وحدة بشكل كامل.
- راجع التمارين وقوائم التحقق بعد كل وحدة.
- فكر في إعادة زيارة الأقسام لتعزيز الفهم.

التعليمات

- اقرأ كل وحدة بعناية ودوّن الملاحظات.
- أكمل التمارين لتطبيق معرفتك.
- استخدم المعجم للمصطلحات غير المألوفة.
- شارك في اختبار الذات لتقييم فهمك.
- راجع الملخص ذي الصفحة الواحدة للنقاط الرئيسية.
- ابقَ على اطلاع بممارسات الأمان مع تطورها.

تم تصميم هذه الدورة لتكون قابلة للطباعة للدراسة دون اتصال بالإنترنت.

احتفظ بمذكرات لتعلمك وتجاربك الشخصية في الأمان.

حدد جدولًا منتظمًا لمراجعة مواد الدورة.

فهرس المحتويات

انقر على عناوين الوحدات للتنقل مباشرة إلى الأقسام.

مقدمة / توجيه

لمن هذا الكورس

- المبتدئون الذين يرغبون في أساس قوي في ممارسات الأمان.
- المستخدمون المتعلمون ذاتيًا الذين يبحثون عن معرفة منظمة حول الاحتيالات والأمان.
- الأفراد المهتمون بحماية أصولهم الرقمية.

ماذا ستتعلم

- تحديد أنواع مختلفة من الاحتيالات ومحاولات التصيد.
- فهم تكتيكات الهندسة الاجتماعية التي يستخدمها المحتالون.
- تنفيذ نظافة الحفظ لحماية أصولك.
- التعرف على أهمية نهائية المعاملات.
- بناء مجموعة أمان شخصية لتداول أكثر أمانًا.
- تطوير عادات التحقق لتجنب الاحتيالات.

ما لن يفعله هذا الكورس

- تقديم نصائح أو توصيات استثمارية محددة.
- ضمان الأرباح أو النجاح في التداول.
- استبدال الحاجة إلى التعليم المستمر في ممارسات الأمان.
- تقديم استراتيجيات تداول أو استثمار في الوقت الحقيقي.

المتطلبات المسبقة

- لا يتطلب معرفة سابقة.
- رغبة في التعلم وتطبيق ممارسات الأمان.

فهم فئات الاحتيال

الهدف: لتعريف المتعلمين بأنواع مختلفة من الاحتيالات الشائعة في أسواق التداول.

احتيالات التصيد

تتضمن احتيالات التصيد خداع الأفراد لتقديم معلومات حساسة، مثل كلمات المرور أو المفاتيح الخاصة، من خلال التظاهر بكيانات موثوقة.

> التصيد: محاولة احتيالية للحصول على معلومات حساسة من خلال التظاهر بمصدر موثوق.

يمكن أن تحدث هذه الاحتيالات عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي أو المواقع الوهمية.

> Hypothetical example
>
> على سبيل المثال، قد يتلقى المستخدم بريدًا إلكترونيًا يبدو أنه من بورصة شرعية يطلب منه التحقق من حسابه من خلال النقر على رابط.

فهم هذه الأنماط أمر حيوي لتجنب الخسائر.

لماذا يهم: التعرف على محاولات التصيد يمكن أن يمنع الوصول غير المصرح به إلى حساباتك.

الاحتيال بالتقمص والإسقاطات الوهمية

تتضمن احتيالات التقمص المحتالين الذين يتظاهرون بأنهم شخص آخر، غالبًا شخصية معروفة في مجال العملات المشفرة، لطلب الأموال أو المعلومات.

> التقمص: التظاهر بأنك شخص آخر لخداع الآخرين.

تعد الإسقاطات الوهمية وعدًا برموز مجانية ولكنها تتطلب من المستخدمين إرسال أموال أو معلومات شخصية.

> Hypothetical example
>
> قد يرى المستخدم منشورًا على وسائل التواصل الاجتماعي يدعي أنه يمنح رموزًا مجانية إذا أرسلوا مبلغًا صغيرًا من العملات المشفرة.

لماذا يهم: الوعي بهذه الاحتيالات يساعد المستخدمين على تجنب الوقوع ضحية لخطط احتيالية.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

قائمة التحقق للوعي بالاحتيال

- تحقق من مصدر أي تواصل قبل التصرف.
- لا تشارك أبدًا مفاتيحك الخاصة أو كلمات المرور.
- كن حذرًا من العروض غير المطلوبة، خاصة تلك التي تعد بعوائد مرتفعة.
- تحقق من الإعلانات الرسمية من المنصات التي تستخدمها.
- استخدم القنوات الرسمية للتحقق من الادعاءات.
- أبلغ عن الأنشطة المشبوهة للسلطات المعنية.
- استمر في تعليم نفسك حول الاحتيالات الجديدة.

تمرين: تحديد أنماط الاحتيال

الغرض: لممارسة التعرف على أنواع الاحتيالات المختلفة في سيناريوهات افتراضية.

1. راجع السيناريوهات المقدمة وحدد أي الاحتيالات موجودة.
2. ناقش مع زميل أو اكتب نتائجك.
3. تأمل في كيفية استجابتك لكل سيناريو.
4. فكر في الإجراءات الوقائية التي يمكنك اتخاذها.
5. شارك أفكارك في مناقشة جماعية.

المخرجات المتوقعة: قائمة بالاحتيالات المحددة والردود المقترحة.

الوعي بالمخاطر

- يمكن أن تؤدي الاحتيالات إلى خسارة كاملة للأموال.
- تحقق دائمًا من صحة الاتصالات.
- كن حذرًا من العجلة والعروض غير المطلوبة.
- استمر في تعليم نفسك بانتظام للبقاء على اطلاع حول الاحتيالات الجديدة.

النقاط الرئيسية

- التصيد والتقمص هما احتيالات شائعة.
- تحقق دائمًا من المصادر قبل مشاركة المعلومات.
- الوعي هو المفتاح لمنع الخسائر.
- ابقَ على اطلاع بأحدث تكتيكات الاحتيال.
- نفذ خطة أمان شخصية.

تقنيات الهندسة الاجتماعية

الهدف: لفهم كيف يقوم المحتالون بالتلاعب بالأفراد للحصول على معلومات حساسة.

العجلة والسلطة

غالبًا ما يخلق المحتالون شعورًا بالعجلة لدفع الأفراد إلى اتخاذ إجراءات سريعة دون تفكير.

> العجلة: تقنية نفسية تضغط على الأفراد للتصرف بسرعة.

قد يتظاهرون بأنهم شخصيات ذات سلطة لكسب الثقة.

> Hypothetical example
>
> قد يدعي المحتال أنه من هيئة تنظيمية ويحتاج إلى التحقق الفوري من هويتك.

لماذا يهم: التعرف على هذه التكتيكات يمكن أن يساعدك على التوقف والتحقق قبل التصرف.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

خطافات المكافآت

غالبًا ما يستخدم المحتالون وعد المكافآت لجذب الأفراد.

> خطاف المكافأة: تقنية تقدم شيئًا مرغوبًا للتلاعب بالسلوك.

يمكن أن تؤدي هذه الخطافات إلى مشاركة معلومات حساسة.

> Hypothetical example
>
> قد يتلقى المستخدم رسالة تدعي أنه قد فاز بجائزة ولكن يجب عليه تقديم معلومات شخصية للمطالبة بها.

لماذا يهم: الوعي بهذه الخطافات يمكن أن يمنعك من الوقوع في الاحتيالات.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

قائمة التحقق للوعي بالهندسة الاجتماعية

- كن مشكوكًا في الاتصالات غير المطلوبة.

- تحقق من ادعاءات العجلة أو السلطة.
- تجنب مشاركة المعلومات الشخصية دون تحقق.
- تعرف على علامات خطافات المكافآت.
- استمر في تعليم نفسك حول تقنيات الهندسة الاجتماعية الشائعة.
- ناقش هذه التكتيكات مع الزملاء لتعزيز التعلم.
- ابقَ على اطلاع حول تقنيات التلاعب الجديدة.

تمرين: تحليل سيناريوهات الهندسة الاجتماعية

الغرض: لممارسة التعرف على تكتيكات الهندسة الاجتماعية في حالات افتراضية.

1. راجع السيناريوهات المقدمة وحدد التكتيكات المستخدمة.
2. ناقش نتائجك مع شريك أو اكتبها.
3. تأمل في كيفية استجابتك لكل سيناريو.
4. فكر في الإجراءات الوقائية التي يمكنك اتخاذها.
5. شارك أفكارك في مناقشة جماعية.

المخرجات المتوقعة: قائمة بتكتيكات الهندسة الاجتماعية المحددة والردود المقترحة.

الوعي بالمخاطر

- يمكن أن تؤدي الهندسة الاجتماعية إلى خسائر مالية كبيرة.
- تحقق دائمًا من هوية الأفراد قبل مشاركة المعلومات.
- كن حذرًا من الطلبات العاجلة للمعلومات.
- استمر في تعليم نفسك بانتظام حول تقنيات التلاعب.

النقاط الرئيسية

- العجلة والسلطة هما تكتيكان شائعان للتلاعب.
- يمكن أن تؤدي خطافات المكافآت إلى مشاركة معلومات حساسة.
- الوعي هو المفتاح لمنع احتيالات الهندسة الاجتماعية.
- ابقَ على اطلاع بأحدث التكتيكات التي يستخدمها المحتالون.
- نفذ خطة أمان شخصية.

ممارسات نظافة الحفظ

الهدف: لفهم كيفية حماية أصولك الرقمية من خلال ممارسات الحفظ المناسبة.

فهم مخاطر الحفظ

تشير الحفظ إلى إدارة وحماية الأصول الرقمية.

> الحفظ: المسؤولية عن حماية الأصول.

يمكن أن تحدث الخسائر من خلال الاختراقات أو الاحتيالات أو الإهمال.

> Hypothetical example
>
> قد يفقد المستخدم أموالًا إذا تم اختراق حسابه في البورصة.

لماذا يهم: فهم مخاطر الحفظ يساعدك على اتخاذ تدابير استباقية لحماية أصولك.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

تقليل سطح الهجوم

يتضمن تقليل سطح الهجوم تقليل الثغرات.

> سطح الهجوم: مجموع الثغرات في نظام ما.

يمكن تحقيق ذلك من خلال ممارسات وأدوات آمنة.

> Hypothetical example
>
> استخدام محفظة أجهزة يقلل من خطر الاختراقات عبر الإنترنت.

لماذا يهم: يعني سطح الهجوم الأصغر فرصًا أقل للمحتالين.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

قائمة التحقق لنظافة الحفظ

- استخدم كلمات مرور قوية وفريدة لجميع الحسابات.

- قم بتمكين المصادقة الثنائية (2FA) حيثما أمكن.
- فكر في استخدام محافظ الأجهزة للتخزين على المدى الطويل.
- راجع وحدث ممارسات الأمان الخاصة بك بانتظام.
- كن حذرًا من مشاركة الوصول إلى حساباتك.
- استمر في تعليم نفسك حول أفضل ممارسات الحفظ.
- ابقَ على اطلاع حول أدوات وتقنيات الأمان الجديدة.

تمرين: تقييم ممارسات الحفظ الخاصة بك

الغرض: لتقييم ممارسات الحفظ الحالية الخاصة بك وتحديد مجالات التحسين.

1. راجع طرق وأدوات الحفظ الحالية الخاصة بك.
2. حدد الثغرات المحتملة في ممارساتك.
3. ناقش مع زميل أو اكتب نتائجك.
4. فكر في التغييرات التي يمكنك إجراؤها لتعزيز الأمان.
5. شارك أفكارك في مناقشة جماعية.

المخرجات المتوقعة: قائمة بالثغرات المحددة والتحسينات المقترحة.

الوعي بالمخاطر

- يمكن أن تؤدي مخاطر الحفظ إلى خسارة كاملة للأصول.
- استخدم دائمًا طرقًا آمنة لإدارة أصولك.
- كن حذرًا من مشاركة الوصول إلى حساباتك.
- استمر في تعليم نفسك بانتظام حول أفضل ممارسات الحفظ.

النقاط الرئيسية

- فهم الحفظ أمر حيوي لحماية الأصول.
- تقليل سطح الهجوم يقلل من المخاطر.
- تنفيذ ممارسات أمان قوية أمر ضروري.
- ابقَ على اطلاع حول نظافة الحفظ.
- راجع تدابير الأمان الخاصة بك بانتظام.

شرح نهائية المعاملات

الهدف: لفهم مفهوم نهائية المعاملات وتأثيراتها.

ما هي نهائية المعاملات؟

تشير نهائية المعاملات إلى النقطة التي لا يمكن فيها عكس المعاملة.

> نهائية المعاملة: الحالة غير القابلة للعكس لمعاملة مكتملة.

بمجرد التأكيد، تكون المعاملات على شبكات البلوكشين دائمة.

> Hypothetical example
>
> إذا أرسلت عملة مشفرة إلى عنوان خاطئ، فلا يمكن استردادها.

لماذا يهم: فهم النهائية يساعدك على اتخاذ قرارات مستنيرة قبل تنفيذ المعاملات.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

تأثيرات النهائية

تتطلب الطبيعة غير القابلة للعكس للمعاملات الحذر.

> غير القابل للعكس: حالة لا يمكن التراجع عنها.

يمكن أن تؤدي الأخطاء إلى خسائر دائمة.

> Hypothetical example
>
> إرسال أموال إلى عنوان محتال يؤدي إلى خسارة كاملة.

لماذا يهم: الوعي بنهاية المعاملات يمكن أن يمنع الأخطاء المكلفة.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

قائمة التحقق للوعي بنهاية المعاملات

- تحقق من العناوين قبل إرسال الأموال.

- افهم تأثيرات المعاملات غير القابلة للعكس.
- كن حذرًا عند تنفيذ المعاملات، خاصة مع المبالغ الكبيرة.
- استمر في تعليم نفسك حول عمليات المعاملات.
- ابقَ على اطلاع حول تكنولوجيا البلوكشين.
- ناقش نهائية المعاملات مع الزملاء لتعزيز التعلم.
- راجع فهمك لعمليات المعاملات بانتظام.

تمرين: تحليل سيناريوهات المعاملات

الغرض: لممارسة تقييم نهائية المعاملات في حالات افتراضية.

1. راجع السيناريوهات المقدمة.
2. حدد المخاطر والأخطاء المحتملة في كل سيناريو.
3. ناقش نتائجك مع شريك أو اكتبها.
4. فكر في الإجراءات الوقائية التي يمكنك اتخاذها.
5. شارك أفكارك في مناقشة جماعية.

المخرجات المتوقعة: قائمة بالمخاطر المحددة والردود المقترحة.

الوعي بالمخاطر

- يمكن أن تؤدي نهائية المعاملات إلى خسارة كاملة للأموال.
- تحقق دائمًا من تفاصيل المعاملة قبل التنفيذ.
- كن حذرًا من المعاملات غير القابلة للعكس.
- استمر في تعليم نفسك بانتظام حول عمليات المعاملات.

النقاط الرئيسية

- نهائية المعاملات مفهوم حاسم في التداول.
- يمكن أن تؤدي المعاملات غير القابلة للعكس إلى خسائر كبيرة.
- الوعي هو المفتاح لمنع الأخطاء المكلفة.
- ابقَ على اطلاع حول عمليات المعاملات.
- نفذ عملية مراجعة شخصية قبل المعاملات.

بناء مجموعة الأمان

الهدف: لفهم مكونات مجموعة الأمان الشخصية للتداول الآمن.

مدراء كلمات المرور

تساعد مدراء كلمات المرور في تخزين وتوليد كلمات مرور قوية بشكل آمن.

> مدير كلمات المرور: أداة تخزن وتشفّر كلمات المرور.

يقلل استخدام مدير كلمات المرور من خطر كلمات المرور الضعيفة.

> Hypothetical example
>
> يمكن للمستخدم توليد كلمات مرور معقدة لكل حساب دون الحاجة إلى تذكرها.

لماذا يهم: كلمات المرور القوية ضرورية لحماية الحسابات.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

المصادقة الثنائية (2FA)

تضيف 2FA طبقة إضافية من الأمان من خلال طلب شكل ثانٍ من التحقق.

> المصادقة الثنائية: عملية أمان تتطلب شكلين من التعريف.

هذا يجعل الوصول غير المصرح به أكثر صعوبة.

> Hypothetical example
>
> يجب على المستخدم إدخال رمز يتم إرساله إلى هاتفه بالإضافة إلى كلمة المرور.

لماذا يهم: تعزز 2FA بشكل كبير أمان الحساب.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

محافظ الأجهزة

تخزن محافظ الأجهزة العملات المشفرة دون اتصال، مما يوفر أمانًا معززًا.

> محفظة الأجهزة: جهاز مادي يخزن العملات المشفرة بشكل آمن.

تحمي من الاختراقات عبر الإنترنت.

> Hypothetical example
>
> يمكن للمستخدم تخزين أصوله في محفظة أجهزة، مما يجعلها أقل عرضة للتهديدات عبر الإنترنت.

لماذا يهم: استخدام محفظة أجهزة يمكن أن يمنع الوصول غير المصرح به إلى أموالك.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

قائمة التحقق لمجموعة الأمان

- استخدم مدير كلمات المرور لجميع الحسابات.
- قم بتمكين 2FA على كل منصة تقدم ذلك.
- فكر في الاستثمار في محفظة أجهزة للتخزين على المدى الطويل.
- قم بتحديث كلمات المرور وإعدادات الأمان الخاصة بك بانتظام.
- استمر في تعليم نفسك حول أحدث أدوات وتقنيات الأمان.
- ناقش ممارسات الأمان مع الزملاء لتعزيز التعلم.
- ابقَ على اطلاع حول التهديدات والثغرات الجديدة.

تمرين: بناء مجموعة الأمان الخاصة بك

الغرض: لإنشاء مجموعة أمان شخصية تناسب احتياجاتك.

1. قيم ممارسات الأمان الحالية الخاصة بك.
2. حدد الفجوات في مجموعة الأمان الخاصة بك.
3. ابحث واختر الأدوات لتعزيز أمانك.
4. أنشئ خطة لتنفيذ هذه الأدوات.
5. شارك مجموعة الأمان الخاصة بك مع زميل للحصول على تعليقات.

المخرجات المتوقعة: خطة شاملة لمجموعة الأمان تناسب احتياجاتك.

الوعي بالمخاطر

- يمكن أن تؤدي مجموعة الأمان الضعيفة إلى خسارة كاملة للأموال.
- استخدم دائمًا كلمات مرور قوية و2FA.
- كن حذرًا من مشاركة الوصول إلى حساباتك.
- استمر في تعليم نفسك بانتظام حول ممارسات الأمان.

النقاط الرئيسية

- مجموعة الأمان القوية ضرورية للتداول الآمن.
- مدراء كلمات المرور و2FA تعزز الأمان بشكل كبير.
- راجع وحدث ممارسات الأمان الخاصة بك بانتظام.
- ابقَ على اطلاع حول أدوات وتقنيات الأمان الجديدة.
- نفذ خطة أمان شخصية.

عادات التحقق

الهدف: لتطوير عادات تحقق جيدة لتجنب الاحتيالات.

التحقق من الروابط

تحقق دائمًا من الروابط قبل النقر لتجنب مواقع التصيد.

> التحقق من الروابط: عملية التحقق من صحة عنوان URL.

يمكن أن يكشف تمرير الماوس فوق الروابط عن وجهتها الحقيقية.

> Hypothetical example
>
> قد يتلقى المستخدم رابطًا يبدو شرعيًا ولكنه يؤدي إلى موقع احتيالي.

لماذا يهم: التحقق من الروابط يمكن أن يمنع الوقوع ضحية للاحتيالات.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

الأذونات والموافقات

راجع دائمًا الأذونات قبل منح الوصول إلى حساباتك.

> الأذونات: الحقوق الممنوحة للتطبيقات أو المستخدمين للوصول إلى معلوماتك.

كن حذرًا من التطبيقات التي تطلب أذونات مفرطة.

> Hypothetical example
>
> قد يطلب تطبيق شرعي الوصول إلى جهات الاتصال الخاصة بك، لكن قد يطلب تطبيق احتيالي أذونات غير ضرورية.

لماذا يهم: مراجعة الأذونات تساعد في حماية بياناتك وأصولك.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

قائمة التحقق لعادات التحقق

- تحقق دائمًا من الروابط قبل النقر.

- راجع الأذونات قبل منح الوصول.
- استمر في تعليم نفسك حول تكتيكات التصيد الشائعة.
- كن حذرًا من الطلبات غير المطلوبة للمعلومات.
- ناقش عادات التحقق مع الزملاء لتعزيز التعلم.
- ابقَ على اطلاع حول تقنيات التحقق الجديدة.
- راجع ممارسات التحقق الخاصة بك بانتظام.

تمرين: ممارسة تقنيات التحقق

الغرض: لتعزيز عادات التحقق الجيدة في سيناريوهات افتراضية.

1. راجع السيناريوهات المقدمة وحدد فرص التحقق.
2. ناقش نتائجك مع شريك أو اكتبها.
3. تأمل في كيفية استجابتك لكل سيناريو.
4. فكر في الإجراءات الوقائية التي يمكنك اتخاذها.
5. شارك أفكارك في مناقشة جماعية.

المخرجات المتوقعة: قائمة بفرص التحقق المحددة والردود المقترحة.

الوعي بالمخاطر

- يمكن أن تؤدي عادات التحقق الضعيفة إلى خسائر كبيرة.
- تحقق دائمًا من الروابط والأذونات قبل التصرف.
- كن حذرًا من الطلبات غير المطلوبة للمعلومات.
- استمر في تعليم نفسك بانتظام حول ممارسات التحقق.

النقاط الرئيسية

- عادات التحقق الجيدة ضرورية للأمان.
- تحقق دائمًا من الروابط والأذونات قبل التصرف.
- الوعي هو المفتاح لمنع الاحتيالات.
- ابقَ على اطلاع حول أحدث تقنيات التحقق.
- نفذ عملية مراجعة شخصية للتحقق.

إجراءات التشغيل القياسية للأمان الشخصي

الهدف: لتطوير إجراء تشغيل قياسي للأمان الشخصي.

إنشاء إجراءات التشغيل القياسية الخاصة بك

تحدد إجراءات التشغيل القياسية للأمان الشخصي ممارساتك وبروتوكولاتك الأمنية.

> إجراء التشغيل القياسي (SOP): مجموعة من التعليمات خطوة بخطوة للمساعدة في تحقيق نتيجة مرغوبة.

يجب أن تتضمن إجراءات التشغيل القياسية الخاصة بك إرشادات لإدارة كلمات المرور، 2FA، وعادات التحقق.

> Hypothetical example
>
> قد تحدد إجراءات التشغيل القياسية أنك تستخدم دائمًا مدير كلمات المرور وتمكّن 2FA على جميع الحسابات.

لماذا يهم: تساعد إجراءات التشغيل القياسية الواضحة في تعزيز ممارسات الأمان الجيدة.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

تنفيذ إجراءات التشغيل القياسية الخاصة بك

يتضمن تنفيذ إجراءات التشغيل القياسية الخاصة بك وضع إرشاداتك موضع التنفيذ.

راجع وحدث إجراءات التشغيل القياسية الخاصة بك بانتظام حسب الحاجة.

> Hypothetical example
>
> إذا اعتمدت أداة أمان جديدة، قم بتحديث إجراءات التشغيل القياسية الخاصة بك لتشملها.

لماذا يهم: التطبيق المتسق لإجراءات التشغيل القياسية الخاصة بك يعزز الأمان.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

مراجعة إجراءات التشغيل القياسية الخاصة بك بانتظام تضمن فعاليتها.

قائمة التحقق لإجراءات التشغيل القياسية للأمان الشخصي

- أنشئ إجراء تشغيل قياسي للأمان الشخصي يحدد ممارساتك.
- راجع وحدث إجراءات التشغيل القياسية الخاصة بك بانتظام.
- ناقش إجراءات التشغيل القياسية الخاصة بك مع الزملاء للحصول على تعليقات.

- استمر في تعليم نفسك حول ممارسات الأمان الجديدة.
- ابقَ على اطلاع حول التهديدات والثغرات الناشئة.
- نفذ إجراءات التشغيل القياسية الخاصة بك باستمرار.
- تأمل في ممارسات الأمان الخاصة بك بانتظام.

تمرين: تطوير إجراءات التشغيل القياسية للأمان الشخصي

الغرض: لإنشاء إجراءات تشغيل قياسية للأمان الشخصي تناسب احتياجاتك.

1. قم بصياغة إجراءات التشغيل القياسية للأمان الشخصي بناءً على ممارساتك الحالية.
2. حدد مجالات التحسين في إجراءات التشغيل القياسية الخاصة بك.
3. شارك إجراءات التشغيل القياسية الخاصة بك مع زميل للحصول على تعليقات.
4. فكر في التغييرات التي يمكنك إجراؤها لتعزيز الأمان.
5. نفذ إجراءات التشغيل القياسية الخاصة بك وتأمل في فعاليتها.

المخرجات المتوقعة: إجراءات تشغيل قياسية شاملة للأمان الشخصي تناسب احتياجاتك.

الوعي بالمخاطر

- يمكن أن تؤدي عدم وجود إجراءات تشغيل قياسية للأمان الشخصي إلى ثغرات.
- راجع دائمًا وحدث إجراءات التشغيل القياسية الخاصة بك حسب الحاجة.
- كن حذرًا من التهديدات الناشئة لأمانك.
- استمر في تعليم نفسك بانتظام حول ممارسات الأمان.

النقاط الرئيسية

- إجراءات التشغيل القياسية للأمان الشخصي ضرورية للممارسات المتسقة.
- تساعد مراجعة إجراءات التشغيل القياسية بانتظام في تعزيز الأمان.
- يمكن أن تمنع إجراءات التشغيل القياسية الخاصة بك الثغرات.
- ابقَ على اطلاع حول أدوات وتقنيات الأمان الجديدة.
- تأمل في ممارسات الأمان الخاصة بك بانتظام.

قائمة التحقق للاستجابة للحوادث

الهدف: لتطوير خطة استجابة للحوادث لخرق الأمان المحتمل.

إنشاء خطة الاستجابة للحوادث الخاصة بك

تحدد خطة الاستجابة للحوادث الخطوات التي يجب اتخاذها في حالة حدوث خرق أمني.

> خطة الاستجابة للحوادث: استراتيجية موثقة للاستجابة للحوادث الأمنية.

يجب أن تتضمن خطتك معلومات الاتصال للإبلاغ عن الحوادث وخطوات للتخفيف من الأضرار.

> Hypothetical example
>
> قد تتضمن خطة الاستجابة للحوادث خطوات لتأمين الحسابات وإبلاغ الأطراف المعنية.

لماذا يهم: وجود خطة يمكن أن يقلل من الأضرار خلال خرق.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

اختبار خطة الاستجابة للحوادث الخاصة بك

يضمن اختبار خطة الاستجابة للحوادث الخاصة بك بانتظام فعاليتها.

قم بإجراء تدريبات لممارسة استجابتك لخرق افتراضي.

> Hypothetical example
>
> قم بمحاكاة هجوم تصيد لاختبار خطة الاستجابة الخاصة بك.

لماذا يهم: يساعد الاختبار في تحديد نقاط الضعف في خطتك.

فهم هذه الأنماط يمكن أن يساعدك في تجنب الخسائر غير الضرورية.

مراجعة خطتك بانتظام تضمن فعاليتها.

قائمة التحقق للاستجابة للحوادث

- أنشئ خطة استجابة للحوادث تحدد خطواتك.
- اختبر خطة الاستجابة للحوادث الخاصة بك بانتظام.
- استمر في تعليم نفسك حول الحوادث الأمنية الشائعة.

- ناقش خطتك مع الزملاء للحصول على تعليقات.
- ابقَ على اطلاع حول التهديدات والثغرات الجديدة.
- نفذ خطة الاستجابة للحوادث الخاصة بك باستمرار.
- تأمل في ممارسات الاستجابة للحوادث الخاصة بك بانتظام.

تمرين: تطوير خطة الاستجابة للحوادث الخاصة بك

الغرض: لإنشاء خطة استجابة للحوادث تناسب الخروقات المحتملة.

1. قم بصياغة خطة الاستجابة للحوادث الخاصة بك بناءً على ممارساتك الحالية.
2. حدد مجالات التحسين في خطتك.
3. شارك خطتك مع زميل للحصول على تعليقات.
4. فكر في التغييرات التي يمكنك إجراؤها لتعزيز الاستجابة.
5. نفذ خطتك وتأمل في فعاليتها.

المخرجات المتوقعة: خطة استجابة شاملة للحوادث تناسب احتياجاتك.

الوعي بالمخاطر

- يمكن أن يؤدي عدم وجود خطة استجابة للحوادث إلى عواقب وخيمة.
- راجع دائمًا وحدث خطتك حسب الحاجة.
- كن حذرًا من التهديدات الناشئة لأمانك.
- استمر في تعليم نفسك بانتظام حول ممارسات الاستجابة للحوادث.

النقاط الرئيسية

- خطة الاستجابة للحوادث ضرورية لإدارة الخروقات.
- يساعد اختبار خطتك بانتظام في تعزيز فعاليتها.
- يمكن أن تقلل تنفيذ خطتك من الأضرار خلال الحوادث.
- ابقَ على اطلاع حول أدوات وتقنيات الأمان الجديدة.
- تأمل في ممارسات الاستجابة للحوادث الخاصة بك بانتظام.

ملخص قواعد ونقاط مراجعة في صفحة واحدة

الممارسات الأمنية الرئيسية

- تحقق دائمًا من الروابط قبل النقر.
- استخدم كلمات مرور قوية وفريدة ومدير كلمات مرور.
- قم بتمكين 2FA على جميع الحسابات.
- راجع وحدث ممارسات الأمان الخاصة بك بانتظام.

الوعي بالاحتيالات

- كن حذرًا من الاتصالات غير المطلوبة.
- تعرف على أنماط الاحتيال الشائعة.
- استمر في تعليم نفسك حول الاحتيالات الجديدة بانتظام.
- أبلغ عن الأنشطة المشبوهة.

الاستجابة للحوادث

- أنشئ واختبر خطة استجابة للحوادث.
- ابقَ على اطلاع حول التهديدات الناشئة.
- تأمل في ممارسات الأمان الخاصة بك بانتظام.
- نفذ خطتك باستمرار.

أفكار نهائية

- الأمان عملية مستمرة.
- ابقَ على اطلاع وقابل للتكيف.
- تفاعل مع المجتمع للتعلم المشترك.
- أعطِ الأولوية لسلامتك الرقمية.

تم تصميم هذا الملخص للرجوع السريع والمراجعة.

المسرد

التصيد

محاولة احتيالية للحصول على معلومات حساسة من خلال التظاهر بمصدر موثوق.

يمكن أن يمنع التعرف على محاولات التصيد الوصول غير المصرح به إلى حساباتك.

الحفظ

المسؤولية عن حماية الأصول.

يساعد فهم مخاطر الحفظ على اتخاذ تدابير استباقية لحماية أصولك.

المصادقة الثنائية (2FA)

عملية أمان تتطلب شكلين من التعريف.

تعزز 2FA بشكل كبير أمان الحساب.

خطة الاستجابة للحوادث

استراتيجية موثقة للاستجابة للحوادث الأمنية.

يمكن أن يقلل وجود خطة من الأضرار خلال خرق.

سطح الهجوم

مجموع الثغرات في نظام ما.

يعني سطح الهجوم الأصغر فرصًا أقل للمحتالين.

إجراء التشغيل القياسي (SOP)

مجموعة من التعليمات خطوة بخطوة للمساعدة في تحقيق نتيجة مرغوبة.

تساعد إجراءات التشغيل القياسية الواضحة في تعزيز ممارسات الأمان الجيدة.

التحقق من الروابط

عملية التحقق من صحة عنوان URL.

يمكن أن يمنع التحقق من الروابط الوقوع ضحية للاحتيالات.

الأذونات

الحقوق الممنوحة للتطبيقات أو المستخدمين للوصول إلى معلوماتك.

تساعد مراجعة الأذونات في حماية بياناتك وأصولك.

خطاف المكافأة

تقنية تقدم شيئًا مرغوبًا للتلاعب بالسلوك.

يمكن أن يمنع الوعي بهذه الخطافات الوقوع في الاحتيالات.

غير القابل للعكس

حالة لا يمكن التراجع عنها.

يمكن أن يمنع الوعي بنهاية المعاملات الأخطاء المكلفة.

مجموعة الأمان

مجموعة من الأدوات والممارسات لتعزيز الأمان.

مجموعة الأمان القوية ضرورية للتداول الآمن.

التحقق

عملية تأكيد صحة المعلومات أو الطلبات.

عادات التحقق الجيدة ضرورية للأمان.

الهندسة الاجتماعية

تقنيات التلاعب المستخدمة لخداع الأفراد لتقديم المعلومات.

الوعي هو المفتاح لمنع احتيالات الهندسة الاجتماعية.

نظافة الحفظ

ممارسات لإدارة الأصول الرقمية بشكل آمن.

يمكن أن تمنع تنفيذ نظافة الحفظ القوية فقدان الأصول.

احتيال

خطة احتيالية مصممة لخداع الأفراد لتحقيق مكاسب مالية.

يمكن أن يساعد التعرف على الاحتيالات في تجنب الخسائر الكبيرة.

النهائية

الحالة غير القابلة للعكس لمعاملة مكتملة.

يساعد فهم النهائية على اتخاذ قرارات مستنيرة قبل تنفيذ المعاملات.

اختبار الذات

1. ما هو التصيد؟

A. نوع من استراتيجيات الاستثمار

B. محاولة احتيالية للحصول على معلومات حساسة ✓

C. طريقة للتواصل الآمن

D. نوع من العملات المشفرة

شرح: التصيد هو محاولة احتيالية للحصول على معلومات حساسة من خلال التظاهر بمصدر موثوق.

2. ماذا تشير الحفظ في سياق الأصول الرقمية؟

A. عملية تداول الأصول

B. المسؤولية عن حماية الأصول ✓

C. فعل شراء وبيع العملات المشفرة

D. إدارة محافظ الاستثمار

شرح: تشير الحفظ إلى المسؤولية عن حماية الأصول.

3. ما هو الغرض من المصادقة الثنائية (2FA)؟

A. تبسيط إدارة كلمات المرور

B. توفير طبقة إضافية من الأمان ✓

C. إلغاء الحاجة إلى كلمات المرور

D. تتبع نشاط المستخدم

شرح: توفر 2FA طبقة إضافية من الأمان من خلال طلب شكل ثانٍ من التحقق.

4. لماذا من المهم التحقق من الروابط قبل النقر؟

A. لتجنب احتيالات التصيد ✓

B. لزيادة سرعة الإنترنت

C. لتحسين تجربة المستخدم

D. لتقليل استخدام البيانات

شرح: يمكن أن يمنع التحقق من الروابط الوقوع ضحية للاحتيالات.

5. ما هي خطة الاستجابة للحوادث؟

A. استراتيجية لإدارة الاستثمارات

B. استراتيجية موثقة للاستجابة للحوادث الأمنية ✓

C. طريقة لتداول العملات المشفرة

D. خطة للنمو المالي

شرح: خطة الاستجابة للحوادث هي استراتيجية موثقة للاستجابة للحوادث الأمنية.

6. ماذا يعني تقليل سطح الهجوم؟

A. تقليل الثغرات ✓

B. زيادة التعرض للتهديدات

C. تعزيز استراتيجيات التداول

D. توسيع شبكتك

شرح: يعني تقليل سطح الهجوم تقليل الثغرات.

7. ما هو خطاف المكافأة؟

A. تقنية تقدم شيئًا مرغوبًا للتلاعب بالسلوك ✓

B. طريقة لتأمين الحسابات

C. نوع من هجوم التصيد

D. استراتيجية للتداول

شرح: خطاف المكافأة هو تقنية تقدم شيئًا مرغوبًا للتلاعب بالسلوك.

8. ما هو الغرض الرئيسي من إجراء التشغيل القياسي للأمان الشخصي؟

A. لتحديد ممارسات الأمان الخاصة بك ✓

B. لتتبع استثماراتك

C. لإدارة محفظتك التجارية

D. لزيادة الأرباح

شرح: تحدد إجراءات التشغيل القياسية للأمان الشخصي ممارساتك وبروتوكولاتك الأمنية.

9. ماذا تعني نهائية المعاملات؟

A. القدرة على عكس المعاملة

B. الحالة غير القابلة للعكس لمعاملة مكتملة ✓

C. عملية تأكيد المعاملة

D. الوقت الذي يستغرقه إكمال المعاملة

شرح: تشير نهائية المعاملات إلى الحالة غير القابلة للعكس لمعاملة مكتملة.

10. لماذا من المهم اختبار خطة الاستجابة للحوادث بانتظام؟

A. لضمان فعاليتها ✓

B. لزيادة مخاطر الأمان الخاصة بك

C. لتقليل وقت الاستجابة

D. لتحسين مهارات التداول الخاصة بك

شرح: يضمن اختبار خطة الاستجابة للحوادث الخاصة بك بانتظام فعاليتها.

11. ما هو الغرض من مدير كلمات المرور؟

A. لتخزين وتوليد كلمات مرور قوية بشكل آمن ✓

B. لتتبع استثماراتك

C. لإدارة محفظتك التجارية

D. لتحسين استراتيجيات التداول الخاصة بك

شرح: يساعد مدير كلمات المرور في تخزين وتوليد كلمات مرور قوية بشكل آمن.

12. ماذا يجب أن تفعل إذا كنت تشك في محاولة تصيد؟

A. تجاهلها وانتقل إلى الأمام

B. الإبلاغ عنها للسلطات المعنية ✓

C. النقر على الرابط للتحقق

D. مشاركتها مع الأصدقاء

شرح: إذا كنت تشك في محاولة تصيد، أبلغ عنها للسلطات المعنية.

13. ما هي أفضل ممارسة لإدارة الأذونات للتطبيقات؟

A. منح جميع الأذونات لتجنب المشاكل

B. راجع الأذونات قبل منح الوصول ✓

C. تجاهل طلبات الأذونات

D. منح الأذونات فقط للتطبيقات الموثوقة

شرح: تساعد مراجعة الأذونات قبل منح الوصول في حماية بياناتك وأصولك.

14. ما هي أهمية فهم نظافة الحفظ؟

A. يساعد في استراتيجيات التداول

B. يمنع فقدان الأصول من خلال الإدارة الآمنة ✓

C. يزيد من عوائد الاستثمار

D. يبسط عمليات التداول

شرح: يساعد فهم نظافة الحفظ في منع فقدان الأصول من خلال الإدارة الآمنة.

15. ماذا يجب أن تفعل قبل تنفيذ معاملة؟

A. تحقق من تفاصيل المعاملة مرتين ✓

B. تجاهل التفاصيل وامضِ قدمًا

C. اعتمد على الآخرين للتحقق

D. تحقق فقط من المبلغ

شرح: يمكن أن يمنع التحقق من تفاصيل المعاملة قبل التنفيذ الأخطاء المكلفة.