

Mali Kimlik Hırsızlığı Koruması Nedir?

Çalışma Kağıdı

Mali kimlik hırsızlığı koruması, kişisel verileri izleme, güçlü güvenlik uygulamaları ve proaktif dolandırıcılık uyarıları aracılığıyla koruma uygulamasıdır.

Sorular

1. Hırsız SSN'nizi kullanarak kredi kartı açar. Buna ne denir?
A) Hesap devralmak
B) Mali kimlik hırsızlığı
C) Kimlik avı
D) Hacking
2. Hangi koruma adınızda yeni hesaplar açılmasını engeller?
A) Dolandırıcılık uyarısı (7 yıl)
B) Kredi dondusu
C) Şifre yöneticisi
D) 2FA
3. Doğru veya yanlış: Tüm hesaplar için aynı güçlü şifreyi kullanmalısınız.
A) Doğru
B) Yanlış
4. Kimlik avı e-postası aldıysanız bankanızda oturum açmanın en güvenli yolu hangisidir?
A) E-postadaki bağlantıyı tıkla
B) Bankanın URL'sini doğrudan yaz
C) Kaydedilen tarayıcı yer imini kullan
D) Bankanı ara önce
5. Senin adında bilinmeyen bir banka hesabı açıldığını fark ettim. Ne yapmalıyım?
6. E-postanız hacklendi. Mali hesaplarınızı nasıl korursunuz?
7. Bankanızdan olduğunu iddia eden kimlik avı e-postası alıyorum. Yapılacak güvenli şey nedir?
8. Tanımla: Mali kimlik hırsızlığı nedir?
9. Tanımla: Kredi dondusu nedir?
10. Tanımla: Kredi raporunuzu ne sıklıkla kontrol etmelisiniz?

Cevap Anahtarı

1. B) Mali kimlik hırsızlığı — Birinin kişisel verilerini dolandırıcılık için kullanmak kimlik hırsızlığıdır.
2. B) Kredi dondusu — Kredi dondusu, borç verenlerin kredi erişimini engeller ve yeni hesap açılmasını engeller.
3. B) Yanlış — Yanlış — her yerde benzersiz şifreler kullan. Bir başarısızlık sadece o hesabı tehlikeye sokar.
4. B) Bankanın URL'sini doğrudan yaz — E-postadaki bağlantı aracılığıyla asla girilmeyen URL'yi yazarak doğrudan gezin.
5. 1. Bankayı ara ve dolandırıcılık hesabını bildir. 2. FTC'ye kimlik hırsızlığı raporu açın (IdentityTheft.gov). 3. Kredi dosyasında dolandırıcılık uyarısı yerleştir (7 yıl). 4. Krediyi üç büro ile dondur (Equifax, Experian, TransUnion). 5. Ek dolandırıcılık için kredi raporlarını üç ayda bir izle.
6. 1. E-posta şifresini hemen değiştir (güçlü, benzersiz). 2. E-posta ve tüm mali hesaplarda 2FA'yı etkinleştir. 3. Şifre yöneticisini hacked şifreler için kontrol et. 4. Hesap kurtarma seçeneklerini gözden geçir (telefon, yedek e-posta). 5. Yetkisiz erişim için kredi ve banka hesaplarını tara.
7. 1. Bağlantıları tıklamayın veya ekleri indirmeyin. 2. Bankanın web sitesine doğrudan git (URL yaz, e-posta bağlantısını kullanma). 3. Giriş yap ve uyarılar veya yetkisiz erişim için kontrol et. 4. Kimlik avı e-postasını bankanıza ve anti-phishing yetkilerine bildirin (phishing@apwg.org).
8. Kişisel verilerinizin (ad, SSN, kredi kartı) suçlular tarafından dolandırıcılık, hesap açma veya kredi alma için kötüye kullanılması.
9. Krediyi kilitler, böylece hiç kimse (siz dahil) dondurmadan yeni hesap açamaz. Büro başına 0-3 maliyeti yoktur.
10. Yılda en az bir kez (annualcreditreport.com'da ücretsiz). Riskli ise veya şüpheli aktiviteden sonra daha sık kontrol edin.

Bounlu

Tüm kartlar, adım adım çözümler ve AI hoca desteği Notek uygulamasında.
Sınav tarihlerini Promy otomatik hatırlatıcıya çevirir.