

אבטחת מידע

מושגי חובה

מטלחות إلزامية (מושגי حובה).

1. **البصمة الرقمية (Digital Footprint):** مجمل البيانات والأعقاب التي نتركها وراءنا في كل نشاط على شبكة الإنترنت. تتضمن هذه البصمة المواقع التي تصفحنا فيها، المنشورات والصور التي رفعناها، عمليات التسوق عبر الإنترنت، والبيانات التعريفية التي أدخلناها. تُحفظ هذه المعلومات لدى مزودي الإنترنت شركات التكنولوجيا وغالباً ما تُباع لأطراف ثالثة. قد يستغل المهاجمون والجهات المعادية هذه المعلومات لجمع تفاصيل عنا والمس بخصوصيتنا.
2. **التصيد / فيشبنغ (Phishing):** طريقة احتيال شائعة تهدف إلى استدراج وانتزاع معلومات حساسة وشخصية من المستخدمين عبر الشبكة بطرق احتيالية. تتمثل الأهداف المركزية في سرقة أسماء المستخدمين، كلمات المرور، تفاصيل بطاقات الائتمان وأرقام هويات شخصية. يتم تنفيذ التصيد عبر رسائل مزيفة أو روابط ضارة تبدو شرعية تماماً. بمجرد أن يضغط المستخدم على الرابط ويدخل تفاصيله، تنتقل المعلومات بشكل فوري إلى أيدي المهاجمين.
3. **سميشبنغ / التصيد عبر الرسائل النصية (Smishing):** احتيال تصيد يتم تنفيذه بشكل خاص عبر رسائل النص القصيرة (SMS) أو تطبيقات المراسلة. يرسل المهاجمون رسائل تحاكي جهات معروفة مثل البريد، البنوك أو شركات الائتمان. تحتوي الرسائل غالباً على عنصر ضغط أو استعجال والضغط على رابط مزيف. قد يؤدي الضغط على الرابط إلى سرقة معلومات مالية أو تنزيل ملفات ضارة.
4. **فيشبنغ صوتي / التصيد الصوتي (Vishing):** نوع من التصيد يحدث عبر مكالمات هاتفية صوتية Voice Phishing في إطار هذه المكالمة، انتحل المهاجم شخصية موظف بنك، شركة تجارية أو جهة حكومية. يحاول المنتحل كسب ثقة الضحية لاختلاس رموز سرية، كلمات مرور أو تفاصيل بطاقات ائتمان. قد يسلم الضحية المعلومات من واقع الاعتقاد بأنه يتحدث مع ممثل خدمة شرعي.
5. **الهندسة الاجتماعية (Social Engineering):** تقنية تستغل سلوك الإنسان، براءته أو مشاعره لدفعه نحو تنفيذ أفعال ضارة. لا تعتمد الطريقة على اختراق تكنولوجي، بل على تلاعب نفسي مباشر بالضحية. يستخدم المهاجمون خلق شعور بالإلحاح، الخوف، الفضول أو الإغراء المالي لاكتساب حق الوصول إلى المعلومات. يعتبر هذا العامل البشري بمثابة نقطة الضعف المركزية في أمن المعلومات والسايبير.
6. **برمجيات الفدية (Ransomware):** نوع من البرمجيات الخبيثة التي تتمثل غايتها الأساسية في ابتزاز الأموال من الضحايا عبر الشبكة. بعد اختراقها للجهاز أو الحاسوب، تقوم البرمجية بتشفير الملفات أو قفل الجهاز بالكامل. يطالب المهاجمون الضحية بدفع أموال فدية مالية لقاء تحرير الوصول إلى الملفات أو فك القفل. في أغلب الحالات، حتى بعد دفع الفدية لا توجد ضمانات بأن المعلومات ستُستعاد حقاً.
7. **المصادقة الثنائية / التحقق بخطوتين (Two-Factor Authentication / 2FA):** آلية أمان متقدمة تضيف طبقة حماية إضافية للحسابات الرقمية تتجاوز كلمة المرور العادية. عند تسجيل الدخول، تطلب النظام

تعريفاً إضافياً مثل رمز أحادي الاستخدام يُرسل عبر رسالة نصية (SMS) أو عبر تطبيق مخصص. ونتيجة لذلك، حتى لو حصل طرف خارجي على كلمة المرور الخاصة بك، فلن يتمكن من الدخول إلى الحساب. يوصى بشدة باستخدام هذا التحقق في جميع التطبيقات، شبكات التواصل الاجتماعي وحسابات البنوك.

8. **ملفات (Cookies):** ملفات نصية صغيرة تحفظها المواقع التي نتصفحها على المتصفح أو الجهاز الخاص بنا. تستخدم هذه الملفات لتوثيق تفضيلات التصفح، حفظ المنتجات في سلة التسوق وتحديد هوية المستخدم. مع ذلك، قد تستخدم "الكوكيز" لتتبع شامل لسلوك المستخدم الرقمي عبر الشبكة. إن الموافقة الجارفة على ملفات تعريف الارتباط في مواقع غير معروفة قد تعرض الخصوصية للخطر وتشارك معلومات حساسة.

9. **بروتوكول HTTPS:** بروتوكول اتصال آمن لنقل البيانات بين متصفح المستخدم وموقع الإنترنت. يرمز الحرف S إلى كلمة Secure (مؤمن) ويشير إلى أن المعلومات المنقولة في الموقع مشفرة. يمنع التصفح في موقع ذي عنوان HTTPS طرفاً ثالثاً من الاطلاع على تفاصيل حساسة مثل كلمات المرور والبطاقات الائتمانية. عند تنفيذ عمليات شراء أو إدخال بيانات مالية، يوصى بالتأكد من أن البروتوكول مفعّل وأن رمز القفل يظهر.

10. **إدارة كلمات المرور (Password Manager):** برنامج أو تطبيق آمن مخصص للتخزين، إدارة كلمات مرور قوية ومختلفة. تحفظ المنظومة كلمات المرور كافة بيانات تسجيل الدخول بصورة مشفرة تحت كلمة مرور رئيسية واحدة وفريدة. تلغي هذه الأداة الحاجة إلى تذكر عشرات كلمات المرور المعقدة أو استخدام كلمة مرور ثابتة وضعيفة. يعتبر استخدام هذا البرنامج الطريقة الأكثر توصية وأماناً للحفاظ على الحسابات عبر الشبكة.

11. **أذونات التطبيق (App Permissions):** الصلاحيات التي يمنحها المستخدم لتطبيق قام بتنصيبه للوصول إلى مكونات مختلفة في الجهاز المحمول. قد تتضمن هذه الأذونات الوصول إلى الميكروفون، الكاميرا، جهات الاتصال، الصور والموقع الجغرافي. من المهم فحص كل طلب إذن ومنح الوصول فقط للأمور التي يحتاج إليها التطبيق حقاً. قد يؤدي منح أذونات فائضة لتطبيقات غير معروفة إلى تسريب معلومات شخصية والمس بالخصوصية.

12. **ديب فايك / التزييف العميق (Deepfake):** تكنولوجيا مبنية على الذكاء الاصطناعي لإنتاج مقاطع فيديو، صور أو تسجيلات صوتية مزيفة يستحيل تمييزها عن الواقع. يستخدم المهاجمون التزييف العميق لتقليد شخصيات معروفة، أصدقاء أو أفراد عائلة بغرض الاحتيال. من خلال تزييف الصوت والملاح، يحاول المخترقون إقناع الضحية بتحويل أموال أو تسليم معلومات. تسلط هذه التكنولوجيا الضوء على الحاجة للتحقق المباشر من الهوية وعدم الاكتفاء بالاعتماد على المحتوى البصري فقط.

13. **بطاقة ائتمان مسبقة الدفع (Prepaid Credit Card):** כרטיס נטען بطاقة دفع يتم شحنها مسبقاً بمبلغ مالي محدد ولا تكون مرتبطة بشكل مباشر بحساب البنك. تستخدم هذه البطاقة كأداة آمنة لتنفيذ عمليات الشراء عبر الإنترنت، لا سيما في مواقع جديدة أو غير معروفة. في حال تم كشف تفاصيل البطاقة أو سرقتها، يقتصر الضرر المالي حصرياً على المبلغ المشحون فيها فقط. يُعد هذا حلاً فعالاً لتقليل المخاطر المالية ومنع مدفوعات غير مبرّرة عبر الشبكة.

14. **منظومة السابير الوطنية (מוקד 119):** هيئة حكومية في إسرائيل مسؤولة عن حماية الفضاء المدني من تهديدات السابير والاحتيال عبر الشبكة. تشغل المنظومة مركز بلاغات الطوارئ 119 المتاح لعموم الجمهور

على مدار الساعة. يمكن للمواطنين الذين تعرضوا لحادث، اختراق أو احتيال مالي التوجه لطلب المساعدة والإرشادات. يساعد التوجه السريع للارتباط في تقليل الضرر الشخصي ومنع عوامل أخرى من الوقوع ضحايا.

15. منصة دفع إلكترونية (Online Payment Platform): خدمة رقمية (مثل، Apple Pay، PayPal، Google Pay) تتيح تنفيذ المدفوعات دون كشف بطاقة الائتمان. تربط المنصة بين المشتري والبائع وتنفذ عملية نقل الأموال بصورة آمنة ومشفرة. توفر هذه الخدمات غالباً حماية للمشتري تتيح استرداد الأموال في حالة الاحتيال. يشكل استخدام هذه المنصات بديلاً أكثر أماناً بكثير من تسليم تفاصيل بطاقة الائتمان مباشرة للموقع.