سرقة الحسابات

اختراق الحسابات – من الخلل التقني إلى العنف:

اختراق الحسابات ليس مجرد مشكلة تقنية؛ هو بوابة لعنف أوسع. بمجرد السيطرة على الحساب، يستطيع المعتدي جمع معلومات، مراسلة الآخرين باسم الضحية، أو ابتزازها بمحتوى خاص. كثير من الضحايا لا يربطن بين الاختراق والعنف القائم على النوع الاجتماعي، رغم أن النتيجة واحدة: فقدان السيطرة والشعور بالتهديد.

تعريف اختراق الحسابات:

سرقة الحسابات هي الوصول غير المصرح به إلى حساب رقمي (بريد إلكتروني، حساب تواصل، حساب بنكي، متجر) بحيث يتحكم المهاجم بحسابك أو يستخدمه لإرسال رسائل، سرقة بيانات، ابتزاز.

الهدف قد يكون سرقة أموال، جمع معلومات، انتحال هوية، أو نشر محتوى ضار.

أثر الاختراق على الضحية:

- فقدان بيانات أو سمعة.
- مضايقات أو ابتزاز للآخرين باسم الضحية.
- توتر نفسي وقلق وخوف من التفاعل الرقمي.
- يشعر الضحية بأن حدوده الشخصية قد تم تجاوزها، وقد يتولد شعور دائم بعدم الأمان حتى بعد استعادة الحساب.

كيف تتم عادةً؟

- **التصيد:** رسائل/روابط مزيفة تخدع المستخدم لإدخال بياناته.
- **إعادة استخدام كلمات المرور:** اختراق بيانات من موقع ما وتجربة نفس البيانات في مواقع أخرى.
- **البرمجيات الخبيثة :** برامج تسجّل الضغطات على الكيبورد أو تسرق الملفات.
- **اختراق البريد الاحتياطي/استرداد الحساب:** مهاجم يسيطر على بريدك أو رقمك لاسترجاع حسابات أخرى.
- **سرقة رقم الهاتف :** نقل رقمك إلى شريحة جديدة للحصول على رسائل SMS/رموز استرجاع.
- **الهندسة الاجتماعية:** إقناع جهات دعم المنصات أو أشخاص مقربين بمنح الوصول.

- **ثغرات تطبيقات طرف ثالث :** تفويض تطبيق غير موثوق يمنحه صلاحية على حسابك.

علامات تدل أن حسابك مخترق:

- نشاط او رسائل لم تقومي بها.
- تغيير كلمة المرور أو البريد المرتبط بالحساب دون علمك.
- إشعارات تسجيل دخول من أماكن او أجهزة غريبة.
- فقدان الوصول للحساب (رفض كلمة المرور أو استرجاع عبر بريد غير معروف).
- وصول رسائل "reset password" لم تطلبيها باستمرار.
- أصدقاؤك يتلقون روابط او محتوى غريب صادر من حسابك.

ماذا تفعلين فوراً إذا اشتبهتِ بالاختراق؟

1. افصلي الأجهزة عن الإنترنت مؤقتاً إذا تشكين بوجود برمجية خبيثة.
2. وثّقي الأدلة: صور شاشة لإشعارات الدخول، رسائل التغيير، أي أدلة.
3. حاولي تسجيل الدخول واسترداد الحساب عبر آليات المنصة (استرجاع بكود او بريد احتياطي).
4. غيّري كلمة المرور فوراً للحساب المتأثر ولكل الحسابات الأخرى التي تستخدم نفس كلمة المرور.
5. فعّلي المصادقة الثنائية القوية تطبيق مصادقة أو مفتاح أمني؛ تجنبي SMS إذا أمكن.
6. افحصي جهازك ببرنامج مضادّ برمجيات خبيثة موثوق أو استعيني بخبير تقني.
7. سجّلي الخروج من كل جلسات الدخول من إعدادات الحساب.
8. أبلغي المنصة عن الاختراق واطلبي إغلاق أي نشاط مشبوه واستعادة الحساب.
9. أبلغي الأهل/الأصدقاء/المتلقين إن كان حسابك يرسل طلبات أو روابط خبيثة (حتى لا يقعوا ضحية).
10. استشيري جهة قانونية أو وحدة الجرائم الإلكترونية إذا حصل سرق أموال أو ابتزاز أو تهديد.

❖ **الأمان الرقمي يبدأ بالوقاية**

اختراق الحسابات ليس خللاً تقنياً فحسب، بل تهديد مباشر للأمان الشخصي والخصوصية. استخدام كلمات مرور قوية ومختلفة لكل حساب، وتفعيل التحقق الثنائي، خطوات بسيطة اليوم قد تمنع خسائر كبيرة غداً. الوقاية الرقمية والاستجابة السريعة تقللان الأضرار وتحفظان السيطرة على الحسابات.