انتحال الشخصية

انتحال الشخصية –حين تُسرق هويتك الرقمية

انتحال الشخصية لا يسرق الحساب فقط، بل يسرق الثقة المرتبطة بالاسم والصورة والعلاقات. الضرر هنا مضاعف: الضحية تتأذى، والمحيطون بها قد يُستغلون أو يُخدعون. في حالات كثيرة، يُستخدم الانتحال كمرحلة تمهيدية للابتزاز أو الاحتيال المالي أو التشهير المهني. كلما كانت الهوية الرقمية أوضح وأكثر نشاطاً، زادت احتمالية استهدافها، ما يجعل الحماية المسبقة ضرورة وليس ترفاً.

تعريف انتحال الشخصية:

انتحال الشخصية الرقمية هو اعتداء مباشر على الهوية، حيث يتم سلب الشخص اسمه أو صورته أو حضوره الرقمي، واستخدامه في سياقات لم يخترها ولم يوافق عليها.

أشكال انتحال الشخصية :

- حساب مزيف على منصات التواصل يحمل اسم وصورة الضحية ويكتب باسمها.
- انتحال عبر البريد الإلكتروني إرسال رسائل تبدو وكأنها من الشخص.
- انتحال صوتي أو فيديو استخدام تسجيلات أو تقنيات لتقليد الصوت/الصورة.
- فتح حسابات أو صفحات باسم الضحية لطلب أموال/محتوى أو نشر مواد مسيئة.
- انتحال داخل سياق عمل/مدرسة إرسال رسائل رسمية مزيفة لخلق بلبلة أو ضرر مهني.

السياق الاجتماعي لإنتحال الشخصية:

غالباً ما يُستخدم انتحال الشخصية لاستغلال ثقة الآخرين بالضحية، أو لإيذائها اجتماعياً من خلال مواقف محرجة أو مسيئة تُنسب إليها زوراً.

لماذا يقوم المخترقون أو المتنمرون بانتحال الشخصية؟

- الحصول على ثقة الآخرين للاحتيال أو الابتزاز.
- تشويه سمعة الضحية أو الإساءة إليها.

- الوصول إلى شبكات الضحية وعلاقاتها (صيد معلومات أو نصب).
- الترفيه أو الانتقام أو توجيه حملات مضايقة منظمة.

دوافع الانتحال:

- التشهير أو الانتقام.
- الاحتيال المالي.
- الإيقاع بالآخرين باسم الضحية.

كيف تكتشفي انتحال الشخصية؟

- **تنبيه الأصدقاء أو المتابعين** غالباً يكون أول مؤشر، لأن المنتحل يتواصل مع الآخرين قبل أن تنتبهي أنت.
- **منشورات أو رسائل لم ترسليها** دليل مباشر على أن شخصًاً آخر يستخدم الحساب أو اسمك.
- **إشعارات تسجيل دخول غريبة** علامة تقنية واضحة على اختراق أو محاولة انتحال.
- **طلبات المال أو المعلومات باسمك** من أكثر أساليب الاحتيال انتشاراً.
- **تغيّر السلوك أو النبرة** (عدائية، روابط مشبوهة، محتوى غير معتاد) مؤشر قوي على أن الحساب لم يعد تحت سيطرتك.

ماذا تفعلين فوراً لو اكتشفتِ انتحالاً لشخصيتك أو لشخص تعرفينه؟

1. **وثّقوا الأدلة فوراً**: صور شاشة للملف/المنشورات/الرسائل، روابط، توقيت. لا تمسحوا شيء.
2. **أبلغوا المنصة**: استخدموا آلية التبليغ على فيسبوك/إنستغرام/تويتر/تيك توك... واطلبوا إزالة الحساب لانتحال شخصية.
3. **أخبروا الدائرة القريبة**: أصدقاء/عائلة/زملاء حتى لا يتفاعلوا مع الحساب المزيف.
4. **أمنوا حساباتكم الحقيقية**: غيّروا كلمات المرور، فعّلوا المصادقة الثنائية، وتحققوا من جلسات الدخول المسجلة.
5. **حظر وإبلاغ المتأثرين**: احجبوا الحساب المزيف وبلّغوا كل من تلقى رسائل منه أنّه مزيف.
6. **استشارة فنية/قانونية**: إذا السبب ابتزاز أو تشهير، استشيروا خبير أمان رقمي ومحامٍ/ة أو منظمة حقوقية مختصة.
7. **إشعار رسمي إن لزم**: للجهات المهنية أو المدارس/العمل إن كان الانتحال يؤثر على سمعة أو عمل.

كيف نمنع انتحال الشخصية:

1. **للأفراد**

- استخدمي/ا أسماء مستخدمين فريدة وصعبة التخمين، وفعّلي المصادقة الثنائية.
- لا تنشري معلومات حساسة (مثل رقم الهاتف أو العنوان) بشكل عام.
- اجعلي حساباتك خاصة إذا لا تحتاجين جمهورًا مفتوحاً.
- استخدمي مدير كلمات مرور وغيّري كلمات المرور بانتظام.
- حدّدي من يمكنه رؤية صورك ومنشوراتك عبر إعدادات الخصوصية.
- راقبي ذكر اسمك/صورتك عبر البحث في المنصات بين فترة وفترة.

2. **للمؤسسات/الصفحات العامة**

- سجّلوا أسماء النطاق/العلامة التجارية الرسمية عبر المنصات (Pages verification) عندما يتاح.
- ضعوا سياسة بيان رسمي للتعامل مع حسابات مزيفة (قالب رد، جهة اتصال للإبلاغ).
- علموا الجمهور: انشروا كيف يمكن التمييز بين الحساب الرسمي والمزيف.
- استخدموا أدوات المراقبة والتنبيه عن ذكر العلامة/الاسم.

أثر الانتحال على الضحية:

- فقدان السمعة أو خسائر مهنية.
- مضايقات وابتزاز يستغل الأشخاص الذين يثقون بالهوية المزيفة.
- ضيق نفسي، قلق، وخوف من تواصل الآخرين مع المحتوى المزيف.
- يشعر الضحية بفقدان السيطرة على صورته العامة، وقد يضطر لبذل جهد كبير لتوضيح الحقيقة واستعادة الثقة.

❖ حماية هويتك الرقمية

الهوية الرقمية امتداد للشخصية الحقيقية، وانتهاكها يُعد شكلاً من أشكال العنف. حافظي على خصوصية حساباتك، تحقق من الإعدادات باستمرار، ولا تستجيبي لأي نشاط غريب أو رسائل غير معتادة فوراً. اليقظة الرقمية والاستجابة السريعة عنصران أساسيان للحد من الأضرار واستعادة السيطرة.