



الجمهورية الجزائرية الديمقراطية الشعبية

وزارة البريد والمواصلات السلكية واللاسلكية

تنظم مديرية البريد والمواصلات السلكية
واللاسلكية لولاية مستغانم

تحت إشراف السيد والي ولاية مستغانم

بالتنسيق مع

أمن ولاية مستغانم، المجموعة الإقليمية للدرك الوطني،
جامعة عبد الحميد ابن باديس، مديرية التربية، مديرية
التكوين والتعليم المهنيين، مديرية الشؤون الدينية والأوقاف،
مديرية الثقافة والفنون، مديرية الشباب والرياضة، مديرية
النشاط الاجتماعي والتضامن، المجلس الأعلى للشباب،
الإذاعة الجهوية لمستغانم:

حملة تحسيسية وتوعوية حول المخاطر
المتعلقة باستعمال وسائل التواصل
الاجتماعي
من 04 ماي 2024 إلى 10 ماي 2024



إرشادات للحماية من عمليات النصب والإحتيال

- ضرورة معرفة الرقم الاستعجالي للبنك أو أرقام مراكز النداء.
- وضع بطاقات الدفع الإلكتروني في أماكن آمنة.
- عدم الاحتفاظ بالرمز السري للبطاقة على جهاز الحاسوب أو الهاتف وتجنب إرساله عبر البريد الإلكتروني.
- تفعيل إشعارات الرسائل النصية بخصوص الحساب البريدي أو البنكي للتمكن من تلقي تنبيهات بخصوص أي عملية مالية يتم إجراؤها على حسابك.
- التأكد من ربط بطاقة الدفع برقمك الهاتفي وتغييره في حالة فقده.

في حالة الوقوع ضحية النصب عبر شبكة الأنترنت، يجب
على الفور القيام بالخطوات التالية:

- التقرب إلى أقرب مركز أمني متواجد بمقر الإقامة، مرفوق بدعامة رقمية تحتوي على جميع المعلومات التقنية من: "رسائل إلكترونية، لقطات شاشة، روابط إلكترونية للموقع، الصفحة أو الحساب، أرقام هاتفية، حسابات بريدية أو بنكية" التي كانت بين الضحية و بين المحتال، بالإضافة إلى كل معلومة من شأنها المساعدة في تحديد هوية المحتال.
- التبليغ عن كل حساب أو صفحة تحال على مستعملي شبكة الأنترنت، عبر الموقع الإلكتروني أو صفحات التواصل الاجتماعي الرسمية الخاصة بكل من الدرك الوطني (الموقع ppgn.mdn.dz، الرقم 1055) أو الشرطة (الصفحات تحت اسم الشرطة الجزائرية، الموقع algeriepolice.dz، الرقم 1548، تطبيقه allo (chorta).
- التبليغ عن كل منشور احتيالي بمواقع التواصل الاجتماعي بغية حظره و تفادي وقوع ضحايا آخرين مستقبلا.
- في حالة سرقة المعلومات الشخصية الخاصة ببطاقة الدفع الإلكتروني، يجب على الفور تبليغ المؤسسة المسؤولة عن إصدار البطاقة، من أجل تجميدها وإيقاف الخدمة بها لتفادي خسائر مادية أكثر أو استعمال غير قانوني لها.

إرشادات للحماية من عمليات النصب والإحتيال

- عدم إعطاء المعلومات الشخصية "الاسم واللقب، العنوان الشخصي، رقم بطاقة الائتمان، كلمة السر لحسابات مواقع التواصل الاجتماعي، كلمة السر الموقته أو ما يعرف برمز "OTP"، كلمة السر للحسابات البنكية..."
- عدم إرسال أي صور تتضمن وثائقه الشخصية على غرار "بطاقة التعريف الوطنية، صكوك بريدية أو بنكية، بطاقات الدفع الإلكتروني، جواز السفر، رخصة السياقة"، لتفادي استعمالها في القيام بأعمال غير قانونية يمكن أن تورطه.
- عدم تسديد أي مبلغ لسلة قبل استلامها، خاصة لما يتعلق الأمر بعروض بيع مغرية على مواقع التواصل الاجتماعي (فايسبوك، انستغرام.....إلخ).
- تفضيل الدفع عند استلام السلعة لتجنب الوقوع في الاحتيال، و مكان التسليم يكون في منطقة غير منعزلة حتى لا يتعرض للاعتداء الجسدي و سلب أمواله.
- الحذر من دفع المصاريف المسبقة المشتبه على غرار "مصاريف جمركية، مصاريف قضائية، مصاريف التأمين..."، خاصة الإعلانات المتعلقة بعروض العمل وعروض التأشيرة.....إلخ.
- التحقق من قانونية الشركة أو الهيئة التي يتم التعامل معها على مواقع التواصل الاجتماعي.
- الحذر ثم الحذر من الرسائل الإلكترونية والعروض التي يغلب عليها طابع الاستعجال وتفادي الولوج إلى المواقع المشبوهة.
- عدم الاستجابة التلقائية للروابط التي يتلقاها المواطن سواء في البريد الإلكتروني، الرسائل القصيرة أو حتى من خلال وسائل التواصل الاجتماعي والتي تتمحور أغلبها حول جمع معلومات شخصية. أغلب صفحات الاحتيال تستعمل الإعلان الممول (Sponsor) وهذا لاستهداف أكبر عدد من الضحايا.
- تفعيل ميزة المصادقة الثنائية على مواقع التواصل الاجتماعي لتعزيز أمان الحساب.
- عدم مشاركة البيانات والمعلومات الشخصية.

التسويق الشبكي أو الهرمي:



هذه التقنية تعتمد على إنشاء منصات ومواقع مزيفة عبر شبكة الأنترنت، والتي تقدم نفسها على أنها فروع لشركات عالمية معروفة لها مقر متواجد بالجزائر تعمل في مجال الإستثمار أو تسويق السلع، أين توهم الضحايا بالإشتراك أو المساهمة بمبلغ مالي مقابل أرباح مغرية بالعملة الوطنية وحتى العملة الأجنبية والرقمية، في مقابل قيام الضحية بمهام محددة مسبقا من طرف مسير المنصة، مع إيهامه بزيادة قيمة الأرباح كلما قام بإستقطاب أو تسجيل أشخاص آخرين للإشتراك معه بذات المنصة.

عروض البيع والشراء عبر الانترنت



- انتشار وكثرة المواقع والصفحات والمنصات التي تعرض على المستهلك سلعا وخدمات يكثر عليها الطلب وبأسعار مغرية للغاية،
- لكي ينساق وراءها المشتري، بعدها عند الاتفاق على الثمن والسلعة، يقوم أحد الطرفين بالنصب على الآخر، سواء البائع بحيث يتلقى الثمن دون أن يرسل السلعة وهذا بعد أن يقوم بالتعديل على وصل الإيصال الخاص بإحدى شركات النقل ويرسله للضحية لكي يوهمه أنه أرسل له السلعة، أو العكس بحيث المستهلك يقوم بالتعديل وتزوير وصل البريد الخاص بالبائع ويأخذ السلعة دون دفع الأموال.
- سرقة هويات متسوقي المتاجر الإلكترونية أو بطاقتهم الإنتمائية واستعمال بياناتهم الشخصية في عمليات شراء عبر الأنترنت.
- خطر قرصنة بطاقات الدفع الإلكتروني والمعطيات الشخصية لاسيما عبر الرسائل الإلكترونية مجهولة المصدر، المواقع المزيفة والتطبيقات الإلكترونية أو البرمجيات غير الموثوقة.

مختلف الأساليب المنتهجة في إرتكاب الجرائم الإلكترونية



تقليد الصفحات والمواقع

يستخدم المحتال هذه التقنية بإنشاء صفحة أو موقع مزيف يشبه لدرجة كبيرة الصفحات أو المواقع الرسمية لخداع الضحية وإيهامه بأنه يتواصل مع أطراف معروفة وموثوقة.

تلقي رسائل نصية من أرقام مجهولة أو أجنبية

هذه التقنية تعرف بتلقي الضحية لرسالة نصية من طرف المحتال، تتضمن عرض عمل براتب مغر أو توهيمه بأنه تم اختياره لربح مبلغ مالي معتبر أو سيارة فاخرة، أين يقوم المحتال بالتواصل مع الضحية وتوجيهه للقيام بإجراءات للحصول على الغرض المطلوب، حيث يقوم باستدراجه لدفع مبالغ مالية صغيرة على عدة مراحل تدفع كضرائب أو إتاوة أو مقابل كل خدمة يقدمها المحتال، حتى لا يتفطن الضحية بأنه يتعرض لعملية احتيال.



الإحتيال الثلاثي

تعتمد هذه الطريقة على ثلاثة (03) أطراف هي: "البائع المزيف (المحتال)، البائع الحقيقي (الضحية) والمشتري (الضحية)". أين يقوم المحتال في بادئ الأمر بشراء سلعة أو خدمة من البائع الحقيقي، ويتفق معه على أن التسديد يتم عبر حساب بنكي أو حساب بريدي جاري، ثم يقوم المحتال في المرحلة الموالية بعرض السلعة أو الخدمة عبر مواقع أو منصات التواصل الاجتماعي، ويتفق مع المشتري (الضحية) على إرسال مبلغ السلعة الوهمية عبر حساب بريدي جاري أو حساب بنكي خاص بالبائع الحقيقي، ثم بعد التأكد من أن المشتري دفع المبلغ المالي المتفق عليه، يقوم المحتال بحظر هذا الأخير عبر جميع منصات التواصل الاجتماعي والانسحاب ليورط البائع الحقيقي.

وسائل التواصل الاجتماعي Social Media

تمثل في مختلف التطبيقات والمواقع والمنصات والصفحات الإلكترونية التي تُستخدم للتواصل مع الآخرين، ونشر المعلومات عبر شبكة الإنترنت العالمية من خلال أجهزة الكمبيوتر أو الهواتف المحمولة.

على الرغم مما قد توفره هذه الوسائل من فرص و سهولة للتواصل، يمكن أن تكون أيضًا مجالًا لمختلف التحديات والخلافات، لا سيما فيما يتعلق بالخصوصية والمعلومات الخاطئة والمضايقات السيبرانية والاحتمالات وتأثيرها السلبي على المستخدمين.



مخاطر استعمال وسائل التواصل الاجتماعي

- نصب أو الإحتيال خاصة عمليات الشراء والبيع عبر الانترنت
- الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار
- الإبتزاز و التنمر
- القذف أو السب
- الإهانة أو التشهير
- عروض التوظيف عن بعد
- الأفعال المخالفة للأداب العامة
- جرائم تتعلق بالشخصيات والبيانات المتصلة بالحياة الخاصة
- المساس بأنظمة المعالجة الآلية للمعطيات



أشكال الإحتيال الإلكتروني الأكثر انتشارا في الجزائر

- استغلال فترة التخفيضات والترويج لعروض سلع وخدمات مزيفة على وسائل التواصل الاجتماعي.
- العروض الاحتيالية للعمل داخل وخارج الوطن.
- عروض تسهيل الحصول على التأشيرات (visa).
- عروض الحصول على قروض مالية وكذا البيع بالتقسيط.