حملة تحسيسية حول المخاطر المتعلقة باستعمال الوسائط الاجتماعية من الفترة الممتدة من 04 ماي إلى 10 ماي 2024

Campagne de sensibilisation contre les risques liés à l'utilisation de médias sociaux

مقدمـــة:

تُعرّف وسائل التواصل الاجتماعي (بالإنجليزية : Social Media) بأنّها التطبيقات والمواقع الإلكترونية التي تُستخدم للتواصل مع الآخرين، ونشر المعلومات عبر شبكة الإنترنت العالمية من خلال أجهزة الكمبيوتر أو الهواتف المحمولة، أو أيّة أداة اتصال عبر الإنترنت، وهي تشير عمومًا إلى جميع المواقع ومنصات الويب التي تقدم ما يسمى بالوظائف "الاجتماعية" .
فعلى الرغم من ما قد توفره هذه الوسائط من فرص و سهولة تواصل ، يمكن أن تكون أيضًا مجالًا لمختلف التحديات والخلافات، لا سيما فيما يتعلق بالخصوصية والمعلومات الخاطئة والمضايقات السيبرانية وتأثيرها السلبي على المستخدمين... إلخ

عرفت الجرائم السيبرانية في السنوات الأخيرة تزايد بصفة مستمرة لكن في الآونة الأخيرة، تم رصد العديد من عمليات **التصيد الإلكتروني** استهدفت مستخدمي الأنترنيت، عن طريق نشر إعلانات كاذبة عبر وسائل التواصل الاجتماعي، سواء للتوظيف عن طريق انتحال صفة مختلف الشركات الوطنية، أو عن طريق إغراء الأشخاص بإمكانية ربح جوائز وهدايا قيمة، يكون الهدف من ورائها قرصنة حسابات الجزائريين وسرقة معلوماتهم وبياناتهم الشخصية .

إضافة إلى ظاهرة التصيد الإلكتروني، التي عرفت انتشارا واسعا، تم أيضا تسجيل استفحال ظاهرة النصب والاحتيال والتي خلفت العديد من الضحايا، باستخدام تقنيات **الهندسة الاجتماعية (social engineering)** أو ما يعرف بفن اختراق العقول. هذه التقنية تجعل الضحايا يقومون بعمل ما، أو يصرحون بمعلومات سرية خاصة بهم لصالح المحتال، وهذا بعد كسبه لثقتهم من خلال تواصله معهم عن طريق الهاتف، البريد الإلكتروني أو أي وسيلة للتواصل بغية إتمام عملية الاحتيال.

أنواع القضايا التي تمت معالجتها

- **النصب أو الإحتيال**
- **الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار**
- **الإبتزاز و التنمر**
- **القذف أو السب**
- **الإهانة أو التشهير**
- **عروض التوظيف عن بعد**
- **الأفعال المخالفة للآداب العامة**
- **جرائم تتعلق بالشخصيات والبيانات المتصلة بالحياة الخاصة**
- **المساس بأنظمة المعالجة الآلية للمعطيات**

بعض الإحصائيات:

الدرك الوطني

- عالجت المصالح المختصة في مكافحة الإجرام السيبراني للدرك الوطني خلال سنة 2023، 2473 جريمة سيبرانية، تتقدمها الجرائم الماسة بالحياة الخاصة للأشخاص على غرار الابتزاز، القذف، التشهير والنصب والاحتيال بـ 54 %، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بـ 10%، جرام ضد الشيء العام بـ 30% وجرائم أخرى مختلفة بـ 6% كما تم تسجيل بأن الفئة العمرية الأكثر عرضة للجرائم الإلكترونية هي فئة الشباب من سن 18 الى 32 سنة.
- كما عالج محققو تكنولوجيات الاعلام والاتصال على مستوى الوحدات الإقليمية للدرك الوطني خلال سنة 2023، 917 قضية متصلة بالمعلوماتية، تتقدمها جريمة النصب والاحتيال بـ 364 قضية، الجرائم الماسة بالحياة الخاصة وإفشاء الاسرار بـ162 قضية وجرائم الابتزاز بـ111 قضية.

المديرية العامة للأمن الوطني

- عالجت المصالح المختصة لمكافحة الجرائم السيبرانية بالمديرية العامة للأمن الوطني سنة 2023، 5138 قضية، عولجت منها 4357 قضية بنجاح حيث تم توقيف الفاعلين و تقديمهم امام الجهات القضائية، تقدمتها جرائم المساس بحرمة الحياة الخاصة للأشخاص (السب، الشتم، التهديد، الابتزاز و التشهير) ب 1999 قضية، متبوعة بجرائم النصب والاحتيال ب 1130 قضية .

بعض أشكال الاحتيال الإلكتروني الأكثر انتشارا في الجزائر:

الصور والأساليب المستعملة على الفضاء الافتراضي من طرف المحتالين للإطاحة بضحاياهم، والتي تم استعمالها مؤخرا في الجزائر، نذكر منها:

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

مختلف الأساليب المنتهجة في إرتكاب هذا النوع من الجرائم:

- **<u>تقليد الصفحات والمواقع</u>**

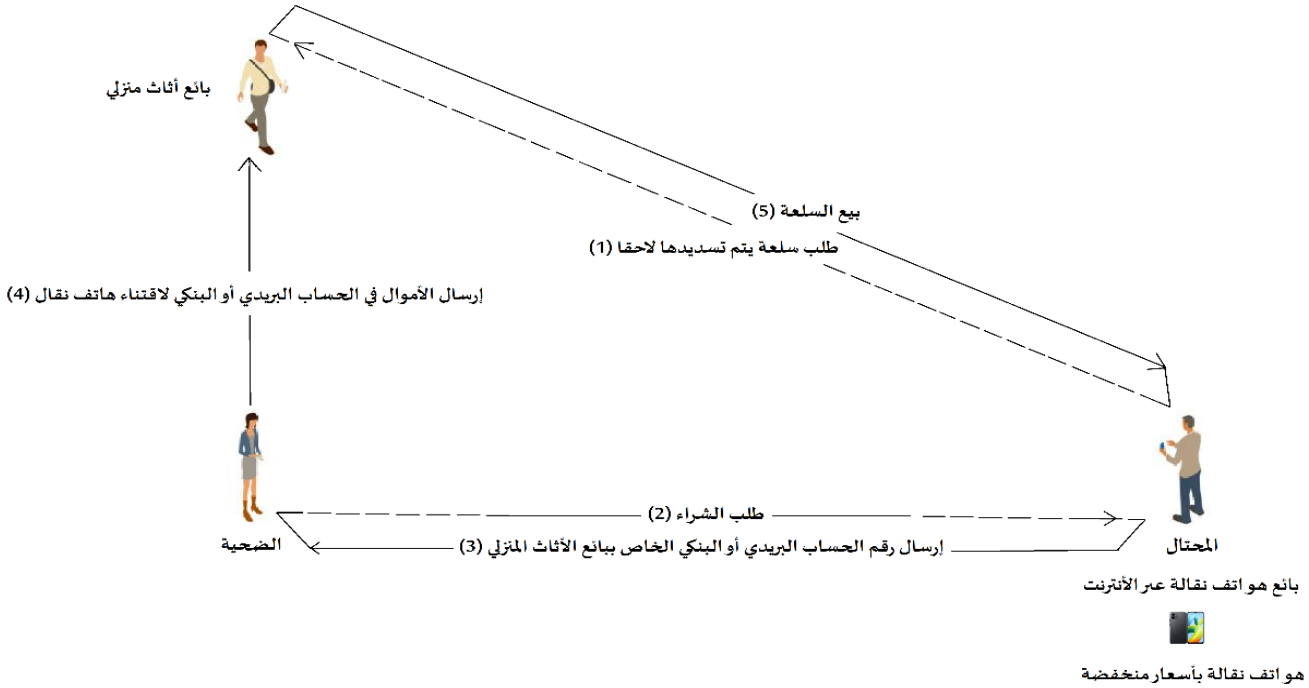
أين يستخدم المحتال هذه التقنية بإنشاء صفحة أو موقع مزيف يشبه لدرجة كبيرة الصفحات أو المواقع الرسمية لخداع الضحية وإيهامه بأنه يتواصل مع أطراف معروفة وموثوقة.

- **<u>تلقي رسائل نصية من أرقام مجهولة أو أجنبية</u>**

هذه التقنية تعرف بتلقي الضحية لرسالة نصية من طرف المحتال، تتضمن عرض عمل براتب مغر أو توهمه 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.

- **<u>الإحتيال الثلاثي</u>**

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 الإجتماعي والانسحاب ليورط البائع الحقيقي.



- **<u>التسويق الشبكي أو الهرمي:</u>** 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 بمهمات محددة مسبقا من طرف مسير المنصة، مع إيهامه بزيادة قيمة الأرباح كلما قام بإستقطاب أو تسجيل أشخاص آخرين للإشتراك معه بذات المنصة.

- **<u>عروض البيع و الشراء عبر الانترنت</u>**

حيث يتم تقديم سلع للبيع بأثمان مغرية لكي ينساق وراءها المواطنون، بعدها عند الاتفاق على الثمن و السلعة، يقوم احد الطرفين بالنصب على الأخر، 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 انه ارسل له السلعة، أو العكس بحيث المستهلك يقوم بالتعديل وتزوير وصل البريد الخاص بالبائع و يأخذ السلعة دون دفع الأموال.

<u>إرشادات للحماية من عمليات النصب والإحتيال:</u>

- من خلال القضايا التي تمت معالجتها، ثبت أن الحلقة الأضعف والسبب الرئيسي في الوقوع في عمليات نصب واحتيال هو المستخدم الالكتروني من خلال جهله من جهة وطمعه من جهة أخرى لذلك يجب التقيد ببعض الإجراءات الوقائية التالية:
- عدم إعطاء المعلومات الشخصية "الاسم والقب، العنوان الشخصي، رقم بطاقة الائتمان، كلمة السّر لحسابات مواقع التواصل الاجتماعي، كلمة السر المؤقتة أو ما يعرف برمز "OTP"،كلمة السّر 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 لسلعة قبل استلامها، خاصة لما يتعلق الأمر بعروض بيع مغرية على مواقع التواصل الاجتماعي (فايسبوك، انستغرام.....إلخ).)الامر هذا لا يخص عمليات التجارة الالكترونية التي تتم ضمن الأطر القانونية)
- 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 المشتبهة على غرار "مصاريف جمركية، مصاريف قضائية، مصاريف التأمين..." ، وهذا في إطار التعامل مع بعض الإعلانات الخاصة مثلا بعروض العمل وعروض التأشيرة .....إلخ.
- التحقق من قانونية الشركة أو الهيئة التي يتم التعامل معها على مواقع التواصل الاجتماعي وهذا عن طريق التأكد بكل الطرق المتاحة.
- الحذر ثم الحذر من الرسائل الإلكترونية والعروض التي يغلب عليها طابع الاستعجال.
- تفادي الولوج الى المواقع المشبوهة.
- عدم الاستجابة التلقائية للروابط التي يتلقاها المواطن سواء في البريد الالكتروني، الرسائل القصيرة أو حتى من خلال وسائط 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.
- تخصيص البروفايل الخاص بحيث لا يرى البيانات سوى أصدقاء المقربين لحامل الحساب.
- وعدم فتح الروابط الإلكترونية الملغمة، التي تحتوي بداخلها فيروسات جاهزة للتثبيت على الجهاز الإلكتروني، على غرار فيروس التتبع (Key Loggers)، حيث بمجرد فتح الرابط الذي يثبت الفيروس على جهاز الكمبيوتر أو الهاتف الذكي بطريقة آلية دون لفت انتباه المستخدم، يعمل على تتبع والتقاط كل المعلومات التي يتم تسجيلها على لوحة المفاتيح وحتى إمكانية موافاة الطرف الآخر بلقطات شاشة لسطح الكمبيوتر أو الهاتف الذكي، التي تستخدم بعدها من قبل قراصنة للحصول على كلمات السر أو مفاتيح التشفير للحسابات البنكية للضحية، أو حتى معلومات شخصية للمستخدم (صور وفيديوهات) يمكن استعمالها من طرف القراصنة لتهديده ثم ابتزازه.
- التبليغ الفوري عن أية جريمة إلكترونية مهما كان طابعها وذلك من خلال الاتصال بأقرب فرقة من فرق الدرك الوطني أو فرقة من فرق الأمن الوطني.
- في حالة الوقوع ضحية النصب عبر شبكة الأنترنت، يجب على الفور 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 هويته.
- التبليغ عن كل حساب أو صفحة تحتال على مستعملي شبكة الأنترنت، عبر الموقع الإلكتروني أو صفحات التواصل الاجتماعي الرسمية الخاصة بكل من الدرك الوطني (الموقع ppgn.mdn.dz ، الرقم1055) أو الشرطة (الصفحات تحت اسم الشرطة الجزائرية، الموقع algeriepolice.dz ، الرقم 1548، تطبيقة allo chorta)
- تبليغ عن كل منشور احتيالي بالمواقع 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 إستعمال غير قانوني لها.

"معا للتوعية من مخاطر الإستعمال السيء للوسائط الإجتماعية"

04 ماي إلى 10 ماي 2024

برنامج الحملة التحسيسية سيتضمن النشاطات التالية:

1- تنظيم دورات ولائية لفائدة السادة الأئمة و السيدات المرشدات الدينيات، قبل انطلاق الحملة التحسيسية بغية تزويدهم بالمعلومات و الإرشادات الوافية حول الموضوع.

2- الإطلاق الرسمي بتاريخ 04 ماي 2024 للحملة عبر تنظيم يوم إعلامي توعوي حول الموضوع.

3- تنظيم نشاطات تحسيسية جوارية على المستوى المحلي لا سيما الجامعات، المدارس، المعاهد العليا، المؤسسات التربوية، مراكز التكوين المهني، المراكز الإسلامية و المدارس القرآنية، دور الثقافة و الشباب و المراكز الثقافية بالتنسيق بين المديرين الولائيين لقطاع البريد و المواصلات السلكية و اللاسلكية و المصالح الخارجية للقطاعات الأخرى المساهمة.

4- تخصيص فضاءات و أجنحة على مستوى الأماكن العمومية بغرض تحسيس المواطنين بمخاطر الإستعمال السيء لشبكات التواصل الإجتماعي و إطلاعهم على وسائل و توصيات الوقاية منها و كذا تبادل التجارب و النقاش.

5-إعداد محتوى تحسيسي رقمي في شكل ومضات مرئية و مسموعة يتم نشره، فضلا عن وسائل الإعلام الوطنية، على صفحات الإنترنت التابعة لدائرتنا الوزارية و على المواقع و الصفحات الرسمية التي تشرف عليها القطاعات الوزارية و الهيئات المتدخلة (على المستويين المركزي و محلي) .

6- جمع و مشاركة تجارب واقعية معاشة لضحايا المخاطر الناجمة عن الوسائط الإجتماعية ،بالتعاون مع المصالح الأمنية المختصة .

7- برمجة خطب و دروس توعوية تتمحور حول موضوع الحملة التحسيسية ،على مستوى مساجد الجمهورية ،يوم الجمعة 10 ماي 2024.

8- ضمان التغطية الإعلامية للنشاطات المسطرة و برمجة تدخلات على الإذاعات المحلية.