

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر.

مقاربة وصفية تحليلية

The role of digital communication in promoting cybersecurity awareness strategies among the internal audience of public institutions in Algeria.

A descriptive and analytical approach.

ط. د فاتح خالدي¹، د. دليلة العوفي²

مخبر وسائل الاتصال والأمن الصحي، جامعة الجزائر 3 (الجزائر)، khaldi.fateh@univ-alger3.dz

² جامعة الجزائر 3 (الجزائر)، laoufi.dalila@univ-alger3.dz

تاريخ النشر: 2026/06/11

تاريخ القبول: 2026/05/31

تاريخ الاستلام: 2026/04/26

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر برفع درجة الوعي السيبراني وترسيخ السلوكيات الآمنة في كيفية التعامل مع المعلومات الحساسة والالتزام بضوابط الأمن السيبراني، مما يضمن حماية الأصول المعلوماتية والرقمية للمؤسسة وهذا لن يتأتى إلا بتسليط استراتيجية التوعية السيبرانية تكون قائمة على التوظيف الفعال للاتصال الرقمي بأدواته وتقنياته المختلفة مما يسمح بتحويل الوعي الذي يتميز به الجمهور الداخلي من مجرد معلومات عامة إلى ثقافة وممارسات يومية تفرض نفسها في وقتنا الراهن الذي يشهد تطورا مذهلا وسريعا في التقنيات الرقمية التي تستخدم في تنفيذ الهجمات السيبرانية. وبالرغم من أهمية الاتصال الرقمي في تعزيز التوعية السيبرانية كإرساء ثقافة التفاعل والتبليغ في حالة رصد المخاطر السيبرانية وتدريب الموظفين في مجال الأمن السيبراني عن طريق دورات تكوينية في إطار بناء القدرات البشرية، إلا أن عدة مؤسسات عمومية لا تحسن استغلال الاتصال الرقمي لتوعية الموظفين في هذا المجال مما يفرض إعادة النظر وبناء استراتيجية شاملة تهدف أساسا إلى تعزيز الثقافة السيبرانية ونشر الوعي في المجال السيبراني.

كلمات مفتاحية: الاتصال الرقمي، الأمن السيبراني، استراتيجية التوعية السيبرانية، الجمهور الداخلي للمؤسسة.

Abstract:

*المؤلف المرسل

This study aims to highlight the role of digital communication in promoting the cyber awareness strategy among the internal audience of the public institution in Algeria by raising the level of cyber awareness and establishing safe behaviors in how to deal with sensitive information and adherence to cyber security controls, which ensures the protection of the institution's information and digital assets. This will only be achieved by outlining a cyber awareness strategy based on the effective use of digital communication with its various tools and technologies, which allows the internal audience's awareness to be transformed from mere general information into a culture and daily practices that impose themselves in our current time, which is witnessing an amazing and rapid development in the digital technologies used to carry out cyber attacks. Despite the importance of digital communication in promoting cyber awareness, such as establishing a culture of interaction and reporting in the event of detecting cyber risks and training employees in the field of cyber security through training courses within the framework of human capacity building, several public institutions do not make good use of digital communication to raise employee awareness in this field, which requires reconsideration and building a comprehensive strategy that aims primarily to promote cyber culture and spread awareness in the cyber field.

Keywords: Digital communication; Cybersecurity; Cyber Awareness Strategy; Internal Audience of the Organization.

مقدمة

تعتمد المؤسسة الحديثة اليوم على الاتصال الرقمي كأحد الركائز الأساسية في إعداد وتنفيذ مهامها الاستراتيجية مما زاد من أهمية الحاجة إلى المعلومات وزيادة تدفقها وحجمها وتراكمها داخل نظام معلومات المؤسسة المفتوح على جمهورها الداخلي أو في علاقتها مع جمهورها الخارجي.

فالاتصال الرقمي لم يعد مقتصرًا على استخدام الوسائط الجديدة أو التكنولوجيا الرقمية، بل أصبح يمثل ثقافة تنظيمية قائمة على التفاعلية والسرعة في تبادل المعلومات في نطاق البيئة المؤسسية، وبالمقابل برزت تحديات عديدة تؤثر على الاتصال الرقمي الآمن للمؤسسة كالتحديات والهجمات السيبرانية، سيما منها التزيف العميق وموثوقية المحتوى الذي يجعلنا لا نميز بين المعلومة الصادرة من الإدارة العليا للمؤسسة والهجمات الذكية التي تطل المؤسسة وجمهورها الداخلي الذي يعتبر في ذاته تهديدًا سيبرانيًا محتملاً يفرض إعداد استراتيجية موجهة خصيصًا له من أجل تحسيسه وتوعيته في المجال السيبراني.

فقد أصبحت التوعية من أهم الأسس التي تبني عليها استراتيجية الأمن السيبراني في المؤسسة، إذ تبين أن العنصر البشري غالبًا ما يكون الحلقة الأضعف في منظومة وسياسة الأمن السيبراني، باعتباره السبب الرئيسي الذي يهدد الأراضية

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر

مقاربة وصفية تحليلية

لارتكاب الهجمات والتهديدات السيبرانية خاصة في ظل ضعف وغياب ثقافة سيبرانية وعدم الوعي والإدراك بالمخاطر والتهديدات التي تطال مؤسسته.

لذلك تبرز الحاجة إلى رفع مستوى وعي الموظفين بأهمية الأمن السيبراني في المؤسسة بما في ذلك القادة وصناع القرار، فقد بات من الضروري إشراك المورد البشري الأساسي في جهود الحماية السيبرانية في سياق الخطط والسياسات المتعلقة بالأمن السيبراني المؤسسي.

إن تمكين الموظفين من المعارف والمهارات الرقمية وتوفير برامج تدريبية وتوعوية منتظمة من شأنها أن تساهم في تطوير وتحسين قدراتهم في التعرف على محاولات الاختيال الإلكتروني، والهجمات المستهدفة من جهة ويساهم في دعم أمن الشبكات وتعزيز جاهزية المؤسسة في مواجهة التهديدات السيبرانية المعقدة والمتغيرة من جهة ثانية.

كما أن إرساء قواعد الوعي بالأمن السيبراني وتعزيز التوعية به وتحسين ممارسات الحماية الرقمية في بيئة العمل أمرا بالغ الأهمية، سيما في ظل التصاعد الكبير لمعدل الهجمات السيبرانية التي تجاوزت نسبتها 100% في بعض القطاعات، وذلك بحسب إحصاءات شركة (point Check) الأمنية لعام 2025.¹ ولم يقتصر الأمر على الهجمات السيبرانية التي تستهدف الأفراد فحسب، فقد شهد عام 2025 انتشارا كبيرا لتنفيذ الهجمات على المؤسسات العمومية منها والخاصة عن طريق استخدام البرمجيات الخبيثة المدعومة بالذكاء الاصطناعي التي تسمح بدمج تقنيات الانتشار والتخفي، وكذا استخدام تقنيات التزييف العميق في عمليات الاختيال وانتحال الهوية.

تبرز هذه المعطيات الحاجة الملحة لبناء ثقافة سيبرانية مؤسسية قائمة على المعرفة والوعي والتدريب، باعتبارها أحد الخطوط الدفاعية الحيوية في مواجهة التهديدات والمخاطر السيبرانية المتنامية مع الاستثمار في برامج التوعية والتكوين المستمر لفائدة الموظفين إلى جانب اعتماد آليات تقنية وإدارية وفنية متكاملة لتعزيز البنية التحتية للأمن السيبراني.

فالتوعية السيبرانية لها أهمية قصوى بالنسبة للمؤسسة سواء كانت عمومية أو خاصة في تعاملاتها المختلفة وفي ممارستها للاتصال الرقمي مع جمهورها الداخلي والخارجي، بهدف حماية مصالحها الرقمية وضمان الاستمرارية في فضاء سيبراني محفوف بالمخاطر وكذا التحديات.

تعمل المؤسسة الجزائرية على ترقية ثقافة الأمن السيبراني وتعزيز التوعية في المجال السيبراني لدى الأفراد مع بناء القدرات في مجال التكوين والتحصين والبحث والتطوير.

تأسيسا لما سبق، أردنا البحث في التساؤل الجوهرى التالي:

¹ علاء الدين حميدي، الأمن السيبراني: خط الدفاع الأول في العصر الرقمي، 2025/12/10،

كيف يساهم الاتصال الرقمي في بناء استراتيجية التوعية السيبرانية لدى الجمهور الداخلي بالمؤسسة العمومية

الجزائرية؟

فككنا هذا التساؤل المحوري إلى التساؤلات الفرعية التالية:

- ✓ ما دور التوعية السيبرانية في الاستراتيجية العامة للأمن السيبراني في المؤسسة العمومية؟
- ✓ كيف يساهم الاتصال الرقمي في تعزيز الوعي السيبراني لدى الجمهور الداخلي للمؤسسة؟
- ✓ ما دور الاتصال الرقمي في بناء ثقافة الأمن السيبراني في المؤسسة؟
- ✓ فيما تتمثل استراتيجية التوعية السيبرانية في المؤسسة العمومية؟

تكتسي هذه الدراسة أهمية بالغة في ظل التحول الرقمي المتسارع الذي تشهده المؤسسات الجزائرية، والذي أفرز تحديات جديدة تتعلق باستخدام آمن وفعال لتقنيات الاتصال الرقمي. فمع تزايد الاعتماد على الوسائط الرقمية في تسير الأعمال والتواصل الداخلي والخارجي، تبرز الحاجة إلى فهم أعمق للعلاقة بين الاتصال الرقمي وتوعية الجمهور الداخلي بالأمن السيبراني.

كما تكمن أهمية هذه الدراسة في إبراز استراتيجية الأمن السيبراني كأولوية وخاصة الاهتمام بالثقافة السيبرانية لدى الموظفين وتأثير ضعفها على العمل الآمن والمسؤول في المؤسسة مما يؤثر على الأداء والاستمرارية، وهذا ما يفرض الاستثمار في رأس المال البشري، من خلال برامج تدريبية وتوعوية تواكب التحول الرقمي وتُعزز مناعة المؤسسة ضد التهديدات السيبرانية المتزايدة.

من الناحية العلمية نجد أن جل الدراسات الموجودة -في حدود اطلاعنا- ركزت على الجانب التقني للأمن السيبراني وغفلت الجانب البشري وأهمية الاتصال في تعزيز حماية معلومات المؤسسات وأمنها.

كما أن الدراسات المتعلقة بالاتصال الرقمي ركزت على الجانب التسويقي والتجاري مع الاهتمام بالصورة الذهنية للمؤسسة لدى جمهورها والحفاظ على سمعتها وتسيير الأزمات التجارية المتعلقة بالصورة والسمعة والعلامة التجارية، في حين غفلت دور الاتصال الرقمي في التوعية والتحسيس والتكوين والكشف عن الثغرات السيبرانية والنظر إلى الاتصال الرقمي من زاوية فعاليته في بناء وتنفيذ استراتيجية الأمن السيبراني على مستوى المستخدمين الداخليين.

حتى نتمكن من تحقيق أهداف الدراسة حاولنا بالتحليل إبراز دور الاتصال الرقمي في تعزيز التوعية السيبرانية وتنفيذها في المؤسسة، بما في ذلك بناء القدرات السيبرانية لجمهورها الداخلي ورفع درجة الوعي لديه بآليات مجاهدة المخاطر السيبرانية دون اغفال دور الاتصال الرقمي في بناء ثقافة الأمن السيبراني في المؤسسة.

المبحث الأول: المفاهيم الأساسية للدراسة وواقع التهديدات السيبرانية على المؤسسة العمومية الجزائرية

المطلب الأول: المفاهيم الأساسية للدراسة

نستعرض أهم المفاهيم التي بنيت عليها الدراسة، بتقديم التعاريف الإجرائية مما يسمح بتبسيط مفهوم التوعية السيبرانية والاستراتيجية التي تتبناها المؤسسة العمومية الجزائرية في مجال الأمن السيبراني.

1. الاتصال الرقمي:

تعددت التعاريف بخصوص الاتصال الرقمي، فقد أطلق عليه البعض من الباحثين الاتصال الإلكتروني، في حين هناك من اختصره في الاتصال عن طريق تطبيقات الواب والذي يعتبر تلك: "العملية الاجتماعية التي يتم فيها الاتصال من بعد، بين أطراف يتبادلون الأدوار في بث الرسالة الاتصالية المتنوعة واستقبالها، من خلال النظم الرقمية ووسائلها لتحقيق أهداف معينة".¹ من خلال دراستنا أردنا أن نبحت في الاتصال الرقمي الذي تلجأ إليه المؤسسة (العمومية)، للاتصال بجمهورها خاصة لتحقيق أهدافها الاتصالية وذلك باستخدام وسائل الاتصال الرقمي، كالبريد الإلكتروني والمراسلات الفورية ومواقع التواصل الاجتماعي ومواقع الواب وتطبيقات الذكاء الاصطناعي، وتطبيقات الهاتف الذكي وغيرها من الخدمات التي تتيحها التكنولوجيا الرقمية، قصد تحقيق التواصل والتفاهم و دعم الثقة والشفافية لدى المؤسسة و جمهورها و بالأخص الداخلي للرفع من الوعي والقدرات السيبرانية لديهم لتمكينهم من أداء مهامهم اليومية المسندة إليهم في مؤسستهم.

2. الأمن السيبراني:

نقصد بالأمن السيبراني تلك الإجراءات العملية والتقنية والإدارية والتنظيمية والاتصالية التي تقوم بها المؤسسة العمومية لحماية أصولها المعلوماتية والرقمية من الوصول أو التعديل أو الحجب غير المرخص لها، بالإضافة إلى الترتيبات وإجراءات الكشف عن الاختراقات والوصول إلى مصادرها في أحسن الظروف للحفاظ على أمنها وثقة جمهورها وسمعتها فيما يتعلق بالخصوصية وحقوق مستخدميها ومتعاملاتها في أبعادها التقنية والاجتماعية والقانونية والتنظيمية والبعد الاتصالي التفاعلي.

3. الثقافة السيبرانية:

تمثل نمط التفكير والسلوك اليومي وجل التقاليد والأعراف داخل الوسط المهني لدى المستخدم الداخلي للمؤسسة العمومية، بما في ذلك درجة الوعي والثقافة التي يملكها في مجال الأمن السيبراني، التي تنعكس وتظهر من خلال استخدام الأجهزة مثل الحاسوب أو الهاتف التي تضمن له الولوج إلى الفضاء السيبراني بطريقة آمنة وواعية مما يضمن له حماية بياناته الشخصية وبيانات مؤسسته.

4. استراتيجية التوعية السيبرانية:

نقصد بها الخطة التي أعدتها المؤسسة العمومية بهدف توعية مستخدميها في مجال الأمن السيبراني انطلاقا من تشخيص حالة الوعي لديهم وكيفية استخدامهم للوسائل الرقمية والتعامل مع الفضاء السيبراني وتهدداته المختلفة.

¹ محمد عبد المجيد، نظريات الإعلام واتجاهات التأثر، 2004، ط3، عالم الكتاب، القاهرة، مصر، ص104.

الاستراتيجية كلمة ارتبط ظهورها بالمجال العسكري، عرفت على أنها فن قيادة الجيش للانتصار من خلال التفكير في الوسائل والسبل التي تسمح بذلك، ويعرفها Porter على أنها: "تركيبة من الأهداف التي تعمل المؤسسة على الوصول إليها، وكذلك الوسائل التي توصلها إلى تحقيق هذه الأهداف".¹

و استراتيجية تعزيز الأمن السيبراني، هي خطة يتم إعدادها مسبقاً، من خلال الاستناد إلى معطيات تم الحصول عليها من أرض الواقع و بناءاً على أهداف مسطرة مسبقاً، توازناً مع المعطيات المطروحة، وهذه الأهداف هناك من هي أهداف رئيسية و فرعية عملية، قريبة و بعيدة المدى تتميز بالدقة و الوضوح و الموضوعية و قابلة للتحقيق ميدانية، حيث يتم تسخير جل الإمكانيات المتاحة من مادية و مالية و بشرية لتحقيق هذه الأهداف الاستراتيجية المسطرة مسبقاً، و يدخل في إطار الاستراتيجية عملية البحث، تخطيط الخطط، الاتصال، الرقابة و المراقبة أو ما يعرف بالمراجعة.

الاستراتيجية الاتصالية أو الإعلامية هي خطة إعلامية يتم إعدادها لتحقيق أهداف محددة، من خلال نقل رسائلها الإعلامية إلى الجمهور المستهدف، لإحداث التأثير المطلوب فيه.²

كما "يشير مفهوم استراتيجية الأمن الوطني السيبراني بشكل عام الى كافة التدابير المتعلقة بسرية المعلومات و البيانات التي يتم معالجتها و تخزينها و إبلاغها عن طريق وسائل إلكترونية أو مشابهة و حمايتها و النظم المرتبطة بها من التهديدات الخارجية أو الداخلية، ففي الوقت الذي يركز مفهوم الحرب التقليدية على استخدام الجيوش النظامية، جاء مصطلح هجمات " الفضاء الإلكتروني" غير محددة المجال أو الأهداف نظراً لتحركها عبر شبكات المعلومات و الاتصالات المتعددة للحدود الدولية أو اعتمادها على أسلحة إلكترونية جديدة تلائم السياق التكنولوجي لعصر المعلومات و التي يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق العملاء لأجهزة الاستخبارات"³

التعزيز يقصد به زيادة الجودة و الفاعلية و القوة و الانتقال من وضعية (أ) إلى وضعية (ب) أفضل، أي تحسين ما هو كائن و تحقيق تحسين عناصر الشيء، ففي الرياضة مثلاً تحقيق رقم قياسي جديد من قبل العداء هو تعزيز لقدراته و ذلك من خلال تطوير تقنيات التدريب و القدرة على التحمل و تحسين السرعة في الأداء و الإتقان، في شق الأمن السيبراني التعزيز يعني التقليل من إمكانية التعرض للاختراق، أي تقليل الفجوة من خلال تطوير آليات رصد المخاطر و توفير تقنيات الدفاع و الردع السيبراني و تطوير البرمجيات المتعلقة بالحماية و السبق السيبراني.

يتم تعزيز الأمن السيبراني من خلال التركيز على المستويات والضوابط المتمثلة في الحوكمة السيبرانية، التعزيز، الصمود، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني للأنظمة.

5. الجمهور الداخلي للمؤسسة العمومية:

¹ صليحة، كاريش، دور أنظمة المعلومات في تنمية القدرة التنافسية للمؤسسة: حالة المؤسسة الجزائرية، رسالة ماجستير، كلية العلوم الاقتصادية، الجزائر، سنة 2000، ص26.

² مي، العبد الله وآخرون، استراتيجيات الإعلام والاتصال في الحروب الراهنة؛ من الحرب الناعمة إلى المواجهة العسكرية، الجامعة اللبنانية، لبنان، 2022، ص 47.

³ راشد حمد النعيمي، العولمة الإعلامية والسياسات الأمنية، الدار العربية للعلوم ناشرون، ط1، بيروت، لبنان، سنة 2020، ص95.

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر

مقاربة وصفية تحليلية

يتمثل الجمهور الداخلي في فئة المستخدمين وتشمل كافة الموظفين من مسؤولين ومسيرين ومؤطرين وإداريين ومدراء وتقنيين وكل من يستخدم تكنولوجيا المعلومات والاتصال ووسائل المعالجة الآلية للمعطيات داخل المؤسسة العمومية في تأدية مهامه خدمة لمصالح المواطنين في إطار الإدارة الإلكترونية.

هناك من يشير إلى الجمهور الداخلي بالمؤسسة بمفهوم المجتمع الداخلي بحيث يراد به¹ "يتمثل المجتمع الداخلي في المشرفين والكتاب والمدراء وحملة الأسهم، المدراء الخارجين"¹

المطلب الثاني: ارتفاع حجم التهديدات السيبرانية التي تطل المؤسسات العمومية

تسعى المؤسسات من خلال استغلالها لمزايا تكنولوجيا المعلومات والاتصال والاستخدام الأمثل للاتصال الرقمي إلى تكثيف نشاطها وحضورها في الفضاء الرقمي بهدف تجسيد أهدافها وأتمتة أعمالها، وبالمقابل تعترضها عدة تهديدات سيبرانية مما يعيق أداء مهامها وتحقيق أهدافها المسطرة.

تعدّ برمجيات الفدية والابتزاز الرقمي من أخطر التهديدات السيبرانية التي تطل المؤسسات نظرا لتداعياتها المالية الخطيرة، وقدرتها على شلّ البنى التحتية الحيوية، وتبرز خطورة هذه البرمجيات بشكل أكبر في الدول الإفريقية، التي تعاني من هشاشة نسبية في أنظمتها السيبرانية الدفاعية، حيث يقوم المهاجم بتشفير بيانات المؤسسة بصفة كلية ويمنع الوصول إليها، ثم يطالب بدفع فدية مالية ضخمة (غالباً بالعملات الرقمية) مقابل فك التشفير. "إذ تشير الأبحاث التي أجرتها شركة الأمن السيبراني Point Check إلى أنه في المتوسط تعرضت 01 من كل 15 مؤسسة في إفريقيا لمحاولة برامج الفدية لكل أسبوع خلال الربع الأول من عام 2023، وهو معدل يفوق المتوسط العالمي، الذي بلغ تقريباً محاولة واحدة لكل 31 مؤسسة أسبوعياً."²

تشهد الجزائر كذلك منحا تصاعديا في التهديدات السيبرانية خاصة، في ظل التحول الرقمي الذي يفرضه الوضع الراهن، إذ تحتل المراتب الأولى عالميا في ترتيب الدول الأكثر تعرضا لمحاولات الاختراق الإلكتروني والهجمات الرقمية، حيث "تم تسجيل خلال عام 2024 نحو 236 039 هجمة إلكترونية عن طريق اكتشاف كلمة السر الخاصة بالحواسيب، و1895 689 هجمة عن طريق استغلال المعلومات الشخصية، و1538 156 هجمة عن طريق المراقبة عن بعد، من خلال متابعة الشخص أو الجهة المستهدفة والتجسس عليها لمحاولة اختراق معلوماتها الرقمية، وهي أرقام عرفت زيادة ملحوظة مقارنة بعام 2023."³

¹ عبد الرزاق محمد الدليمي، المدخل إلى العلاقات العامة، دار الثقافة للنشر والتوزيع، ط1، المملكة الأردنية الهاشمية، سنة 2011، ص135.

² مصطفى جالي، الأمن السيبراني في أفريقيا بين التحديات والرهانات الاستراتيجية، 20 يوليو 2024، ورقة تحليلية، مركز الجزيرة للدراسات، ص4. Sur: stadies.aljazeera.net.

³ زولا سومر، استهداف الجزائر بـ 70 مليون هجمة سيبرانية خلال 10 أشهر، 2024/11/18، يومية المساء، الجزائر. Sur : www.el-massa.com

لقد صنفّت الجزائر ضمن قائمة 20 بلدا الأكثر استهدافا بالهجمات الإلكترونية وهذا ما أكدته مسؤولية منطقة فرنسا وإفريقيا الشمالية والغربية بشركة "كاسبرسكي"، بأن برنامج شركتها المستعمل من طرف عدة مؤسسات بالجزائر أوقف أكثر من 70 مليون "هجمة إلكترونية" ما بين شهري جانفي وأكتوبر 2024، وتعرض ما يقارب 51 % من الحواسيب ذات أنظمة غير آمنة في الجزائر لهجمات تمس بخصوصية المعلومات وأنظمة التشغيل.¹ كما تم حظر أكثر من 13 مليون محاولة تصيد احتيالي وما يقرب من 750,000 مرفق خبيث.²

إذ تتعدد أشكال الهجمات السيبرانية التي تواجه الموظفين في مؤسساتهم، حيث يبرز كل من التصيد الاحتيالي، والهندسة الاجتماعية وهجمات الفدية، والبرمجيات الخبيثة التي تستغل قنوات متنوعة كالبريد الإلكتروني ومنصات التواصل الاجتماعي للإيقاع بهم بالإضافة إلى جرائم الاحتيال الإلكتروني وسرقة الهوية والتجسس الإلكتروني. هذا يستدعي استراتيجية خاصة تعتمد أساسا على حماية كل ما تملكه من بيانات ومعطيات وشبكة اتصالات ومستخدمين في إطار استراتيجية الأمن السيبراني التي تعدّ أولوية للمؤسسات في عصرنا الحالي، ونركز بالخصوص على المستخدمين باعتبارهم الأساس في الاستراتيجية وذلك بالتركيز على توعيتهم سيبرانيا وتعزيز الثقافة السيبرانية لديهم.

المبحث الثاني: دور الاتصال الرقمي في تعزيز الأمن السيبراني لدى الجمهور الداخلي للمؤسسة العمومية الجزائرية

المطلب الأول: التوعية السيبرانية أساس استراتيجية الأمن السيبراني في المؤسسة العمومية الجزائرية

تشير البحوث والتقارير المختلفة إلى أن الجزائر رغم الجهود التي بذلتها في مجال الأمن السيبراني، إلا أنها لاتزال تسجل نقصا وضعفا على مستوى بعض المؤسسات الحكومية من ناحية البنى التحتية الأمنية، نقص في الكفاءات المتخصصة في الأمن السيبراني، تماطل في تحديث الأنظمة بانتظام، نقص الوعي الأمني لدى الموظفين باعتبار الإنسان مصدر التهديدات في معظم الأحيان وذلك عن طريق التحسيس بالمخاطر السيبرانية والتدريب وكذا التوعية السيبرانية.

فالتوعية السيبرانية المستمرة من شأنها أن ترفع من درجة اليقظة والوعي لدى الموظفين، وترسخ لديهم سلوكيات آمنة في التعامل مع البيانات الحساسة ومن المهم أن تصمم هذه البرامج وفق خصوصية كل مؤسسة.³ وتشمل التوعية بالأمن السيبراني في المؤسسة كل المبادرات التي تقوم بها المؤسسة لتشجيع حملات التوعية إلى أكبر عدد من موظفيها ومسؤوليها والاستفادة من مختلف الهيئات والمنظمات وبرامج التعليم والتكوين حتى تصل الرسالة بشأن السلوك الآمن في المجال السيبراني.

فقد أطلقت عدة قطاعات عمومية حملات تحسيسية لأجل تعزيز التوعية في المجال السيبراني باستخدام منصاتها الرقمية

ومواقعها الإلكترونية، نذكر منها على سبيل المثال- لا الحصر-:

¹ لمياء حرزلاوي، 70 مليون هجمة إلكترونية في الجزائر خلال 2024، جريدة الفجر، 2024/11/17-2024/11/17. Sur : alfadjer.dz/article/70-

mlyon-hag-alktrony-fy-algzayr-khal-2024

² التحرير، كاسبرسكي: احباط أكثر من 13 مليون محاولة تصيد احتيالي في الجزائر خلال 2024، دزد شاركتي، 22 مارس 2025.

Sur : dzcharikati.net

³ فارس محمد العمارات، الأمن السيبراني، المفهوم وتحديات العصر، 2022، دار الخليج للنشر والتوزيع، الأردن، ص 7.

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر

مقاربة وصفية تحليلية

الحملة الوطنية التوعوية والتحسيسية التي أطلقتها مؤسسة بريد الجزائر على سبيل المثال التي تسعى إلى تبني استراتيجية أمن سيبراني محكمة من خلال قيامها بإجراءات تقنية إلى جانب تكثيفها للحملات التوعوية للوقاية من الجرائم السيبرانية باستخدام شاشات العرض الإلكترونية داخل مقراتها عبر كامل التراب الوطني ومن خلال موقعها الإلكتروني الرسمي عبر الأنترنت وكذا صفحاتها لمواقع التواصل الاجتماعي عبر محتوى مدروس وجذاب وديناميكي يضمن التفاعل المستمر.

جاءت هذه الحملة تزامنا مع إطلاق وزارة البريد والمواصلات السلكية واللاسلكية أيضا بالتعاون مع الوكالة الوطنية لأمن الأنظمة المعلوماتية من 04 إلى 10 ماي 2024، حملة تحسيسية وتوعوية حول المخاطر المتعلقة باستعمال الوسائط الاجتماعية على مستوى مختلف ولايات الوطن بالتنسيق مع عدة قطاعات وزارية وهيئات أمنية مختصة، بهدف تزويد مستخدمي الوسائط الاجتماعية بالتوصيات الوقائية والممارسات الحميدة الكفيلة بتقليل حدة المخاطر المحدقة بهم في هذه الفضاءات الافتراضية، لاسيما ما تعلق منها بالنصب والاحتيال، علاوة على المساهمة في تلافي آثارها السلبية على تكوين الفرد و الإرث القيمي للمجتمع و تماسك النسيج الأسري والمجتمعي.¹

كما نظمت وزارة البريد والمواصلات السلكية واللاسلكية أيضا، حملة وطنية توعوية وتحسيسية حول النصب والاحتيال عبر الأنترنت تحت شعار "لا تشارك معلوماتك الشخصية عبر الأنترنت. كن يقظا، فالمحتال ينتظر الفرصة " التي نظمتها وزارة البريد والمواصلات السلكية واللاسلكية من 10 الى 30 ماي 2025، بالتنسيق وبمساهمة كل من وزارة الدفاع الوطني، وزارة الداخلية والجماعات المحلية والتهيئة العمرانية، وعدة قطاعات وزارية، بالإضافة إلى الهيئات الأمنية والهيئات المختصة وكذا الوكالة الوطنية لأمن الأنظمة المعلوماتية، حيث تهدف هذه الحملة إلى:²

- ✓ رفع مستوى الوعي لدى المواطنين حول أساليب الاحتيال الإلكتروني الأكثر شيوعا وكيفية التعرف عليها،
- ✓ تزويد المواطنين بالأدوات المعرفية للتصدي لها.
- ✓ تحفيز تبني سلوكيات رقمية آمنة،
- ✓ تشجيع الإبلاغ عن حالات النصب والاحتيال عبر الأنترنت للجهات المختصة.

أطلقت المديرية العامة للأمن الوطني الحملة الإعلامية عبر منصاتها الرقمية، تحت شعار "لسلامتك لا تشارك صورك مع أشخاص لا تعرفهم"، تهدف هذه المبادرة إلى رفع مستوى الوعي المجتمعي بمخاطر مشاركة الصور والمعلومات الشخصية عبر الإنترنت. بما فيهم مستخدمين المؤسسات العمومية، تندرج هذه الحملة ضمن برنامج المديرية العامة للأمن الوطني للتحسيس والتوعية في مجال الأمن السيبراني، الذي تسعى من خلاله إلى تعزيز ثقافة الاستخدام الآمن للتكنولوجيا، وضمان سلامة الأفراد في العالم الرقمي.³

¹ <https://www.mpt.gov.dz/l-حول-وطنية-توعوية-تحسيسية-حملة-اطلاق/> consulté : 15/O6/2025.

² Ibid.

³ https://www.ens-lagh.dz/16_05_2025/ consulté : 13/09/2025.

تهدف هذه الحملات التوعوية إلى رفع مستوى الوعي والمعرفة الرقمية لدى المواطنين بصفة عامة وموظفي المؤسسات العمومية (الجمهور الداخلي) بصفة خاصة، تنفيذاً للاستراتيجية الوطنية للأمن السيبراني وفي إطار الجهود الوطنية المشتركة بين مختلف القطاعات والمؤسسات العمومية لتعزيز الجاهزية لمواجهة تحديات التحول الرقمي مع إشراك المورد البشري الأساسي - الموظفين- في جهود الحماية السيبرانية في سياق الخطط والسياسات المتعلقة بالأمن السيبراني المؤسسي. مع اعتماد برامج تدريب دائمة للموظفين وتعاون أكبر مع الجامعات والمعاهد المختصة واستغلال وسائل الاتصال الرقمي بشكل مكثف لنشر التوعية السيبرانية بين الموظفين والمواطنين.

1. بناء ثقافة الوعي السيبراني لدى الجمهور الداخلي للمؤسسة العمومية

يعتبر الجمهور الداخلي الأساس في تعزيز الأمن السيبراني على مستوى المؤسسة، عن طريق زيادة الوعي بالتهديدات السيبرانية، الأمر الذي يساعدها على الاستجابة في حالة حدوثها.

مسألة بناء ثقافة الوعي السيبراني لا تقتصر على صناع القرار الذين يفرض عليهم الأمر ترجمة المخاطر السيبرانية إلى اتخاذ إجراءات ملائمة، وإنما مسؤولية مشتركة بين كل الأطراف الفاعلة في المؤسسة سيما المستخدمين عن طريق خلق جو من الثقة الرقمية وتحسيسهم بالمخاطر السيبرانية وبدورهم في تأمين بيئة عملهم الرقمية.

فلا يمكن تحقيق حماية المؤسسة من التهديدات السيبرانية بصفة شاملة إلا من خلال رفع مستوى الوعي لدى مستخدميها حول المخاطر ووسائل الوقاية منها. مما يتيح لهم الاستجابة بشكل صحيح وفعال لها، حيث يصبح المستخدمون أكثر قدرة على التعرف على السلوكيات المشبوهة والممارسات غير المشروعة وغير الآمنة.

فقد أثبت الواقع نقص الوعي السيبراني لدى المستخدمين في المؤسسات في ظل التطور المذهل لتكنولوجيا المعلومات والاتصال وارتفاعات الذكاء الاصطناعي، الذي جعل البعض من المستخدمين يعيشون اغتراباً رقمياً ويجدون صعوبة في التعامل مع التقنية هنا يبرز دور المؤسسة في تعزيز القدرات السيبرانية لدى المستخدمين (الجمهور الداخلي) بأدوات وتقنيات مختلفة.

تعد أدوات وتقنيات تعزيز الوعي السيبراني جزءاً أساسياً من استراتيجية التوعية السيبرانية في أي مؤسسة عن طريق برامج التدريب التفاعلية مثل الدروس التعليمية والمحاضرات المسجلة ومنتديات نقاش واختبارات لتقييم مدى استيعابهم لكل المحتويات المتعلقة بالتوعية والتحسيس التي تسمح للمؤسسة بقياس قدرة الفهم والاستيعاب.

2. أهمية الاتصال الرقمي في تعزيز ثقافة الأمن السيبراني في المؤسسة العمومية الجزائرية

يعد تعزيز ثقافة الأمن السيبراني وتحسين ممارسات الحماية الرقمية في بيئة العمل أمراً بالغ الأهمية، سيما في ظل التزايد المضطرد للهجمات السيبرانية التي تستهدف المؤسسات سواء العمومية منها أو الخاصة، حيث تبرز الحاجة الملحة لبناء ثقافة أمنية مؤسسية قائمة على المعرفة والوعي والتدريب، باعتبارها أحد الخطوط الدفاعية الحيوية في مواجهة التهديدات والمخاطر السيبرانية المتنامية. "ثقافة الأمن السيبراني لا تبنى فقط بالتقنيات بل تبدأ بوعي الأفراد والمؤسسات والتزامهم في حماية البيئة الرقمية للمؤسسة"¹

¹ فارس محمد العمارات، مرجع سابق، ص 7.

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر

مقاربة وصفية تحليلية

تحتاج المؤسسة العمومية لبرامج تدريب واسعة وخاصة، ما يسمح لها بزيادة تشجيع تثقيف الموظفين في مجال الأمن السيبراني في مختلف الهياكل والمسؤوليات والمهام مع تنمية مهارات المختصين والخبراء. قد يكون التدريب على مستوى المؤسسة (التدريب الداخلي) بالاستعانة بالمختصين والخبراء الخارجيين في إطار الشراكة مع الهيئات الخاصة الوطنية أو الأجنبية أو خارج المؤسسة (التدريب الخارجي) عن طريق الاستفادة من الدورات التكوينية الوطنية منها والدولية وفق احتياجات المؤسسة في مجال الأمن السيبراني.

يعدّ تدريب الموظفين وتوعيتهم أحد أبرز الممارسات الوقائية التي تعتمد عليها المؤسسات لتعزيز مناعتها الرقمية، ذلك أن التهديدات السيبرانية لا تستهدف نظم المعلومات والشبكات والاتصالات فحسب، بل يتعداها للأفراد، إذ يستغل المهاجمون الثغرات التي تتشكل بسبب السلوك البشري الناتج عن ضعف الوعي أو الجهل بالثقافة السيبرانية لتحقيق أهدافهم، حيث تظهر التقارير أن ما يزيد عن 90 % من الهجمات السيبرانية تعود إلى معلومات تم تسريبها عن غير قصد من قبل المستخدمين داخل المؤسسة باعتبار هذه الفئة من أبرز نقاط الضعف في تعزيز الأمن السيبراني.¹

من هذا المنطلق يعد الموظف محورا أساسيا في تعزيز ثقافة الأمن السيبراني داخل المؤسسة، مما يفرض تمكينه من المعارف والمهارات الضرورية القائمة وتطوير المسارات المهنية لدعم أمن الشبكات الرقمية وتعزيز جاهزية المؤسسة في مواجهة التهديدات السيبرانية المعقدة والمتغيرة.

انطلقت بعض المبادرات الرامية إلى تعزيز الثقافة السيبرانية في الوسط المهني لدى المؤسسات العمومية من خلال تسطير وتنفيذ برنامج وطني لتدريب الموظفين على أساسيات الأمن السيبراني، كما تم عقد عدة دورات تكوينية حول التصيد الاحتيالي وكلمات المرور الآمنة " بالتعاون مع بعض المنظمات الدولية البارزة في المجال كالاتحاد الدولي للاتصالات سعيا منها لبناء القدرات وتدريب الموظفين الحكوميين على أساسيات الأمن السيبراني.²

تسمح مختلف الدورات التدريبية والتكوينية للموظفين وورش العمل التي تشرف عليها مختلف المؤسسات العمومية بتعلم أنواع مختلفة من التهديدات السيبرانية، مثل التصيد الاحتيالي والبرامج الضارة والمحاولات الخبيثة وكيفية التعامل معها بشكل فعال.

فتأتي مبادرة وزارة التكوين والتعليم المهنيين ضمن هذا المسعى بهدف " تأهيل كفاءات تقنية تنفيذية قادرة على الاندماج المباشر داخل المؤسسات، خاصة في المهن التشغيلية المرتبطة بمراقبة الأنظمة المعلوماتية وحمايتها باعتبار التكوين المهني يشكل رافعة أساسية لإعداد تقنيين تنفيذيين قادرين على حماية الأنظمة، تأمين البيانات والمساهمة بفعالية في بناء منظومة رقمية آمنة. " ³

¹ Metacompliance.cyber security awarness and the healthcare. Sur : <https://www.metcompliance.com/blog/cyber-security-awarness>. Consulté : 12/04/2025.

² محمد بلقور، الجزائر في معركة القرن: الأمن السيبراني كجبهة جديدة لحماية الدولة الوطنية، موقع الجزائر الآن، 2025/10/12.

Sur : algeriemaintenant.dz/2025/10/ /الجزائر-في-معركة-القرن-الأمن-السيبراني

³ نسيم أرحاب، الملتقى الوطني حول تعزيز القدرات في مجال الأمن السيبراني، 2022/02/10، النادي الوطني للجيش الجزائر العاصمة.

كما تسمح هذه الدورات التكوينية بتزويد الموظفين بالمهارات اللازمة التي تساعد على التعامل مع تهديدات الفضاء الرقمي، وسبل التصدي لها من خلال قنوات الاتصال المختلفة التي توفرها مؤسسته، فضلا عن النصائح والارشادات حول حماية المعطيات الشخصية واتباع أفضل الممارسات على شكل دليل ارشادي وتوجيهي ينشر على الشبكة الداخلية (أنترانت) أو يرسل عن طريق البريد الإلكتروني للمعنيين.

يمكن ضمان الاتصال بين المستخدمين في إطار جماعات افتراضية يسهر على التنسيق بينهم قائد الفريق، مما يضمن الفعالية والاستمرارية وبالتالي بناء ثقة رقمية بين المستخدم ومؤسسته. فتعزيز الثقافة السيبرانية يمكن المستخدمين من فهم أدوارهم في الحفاظ على الأمن السيبراني مما يعزز من الفعالية الشاملة للجهود الحماية.

لكن رغم الجهود التي بذلتها المؤسسات العمومية في الجزائر في هذا المجال، تبقى بحاجة إلى الرفع من تدريب الموظفين على نطاق واسع وتأهيل الكوادر وتخصيص ميزانيات لا يستهان بها تتماشى والمتطلبات الواقعية للتدريب والتوعية مع وضع استراتيجية شاملة ومتكاملة للتوعية السيبرانية بالاعتماد على الاتصال الرقمي الفعال.

المطلب الثاني: دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية في المؤسسة العمومية

بصفة عامة "الاتصال هو عملية تبادل مستمر في الأفكار والآراء بين شخصين أو أكثر و يكون من خلال اللفظ أو الكتابة، فالقائد في أي مؤسسة أو يدير مجموعة من الأفراد تلتقي إرادتها حول فكرة أو مشروع ما و يشاركون في مسؤولية الاضطلاع بأعمال محددة و تحقيق أهدافها و الاتصال ضروري لأجل الاحتياجات و التطلعات و المشروعات و الأفكار و المبادئ و الأهداف و المصالح و الوسائل المتاحة للمنظمة و يعزز حيويتها و تماسكها و وحدتها كما يجعل كل عضو فيها يشعر قيمته في تحقيق الهدف و بأن يشارك مشاركة فعالة مستوعبا و متفهما مهامها و أعمالها".¹

كما "أصبح الاتصال في القرن الحادي والعشرون قوة هائلة للتأثير في الجماهير، وفي تكوين الرأي العام، وتعديله، لأنه يقوم على أساس فهم الجوانب الإنسانية، لأفراد المجتمع، والمهارة الفنية في الاتصال بالناس والقدرة على رسم الخطط وتنفيذها".² يساهم الاتصال في تعزيز تسطير الاستراتيجيات التي في غالب الأحيان تركز على المدى البعيد، وتتشابه الاستراتيجية بصورة عامة في مكوناتها ومراحلها وطرق بنائها وإعدادها، لكن تختلف من حيث مضمونها وأهدافها، فالأهداف في غالب الأحيان تبقى مفهومة وواضحة لدى الإدارة العليا للمؤسسة مادامت استراتيجية ومحورية في حياتها مما يضمن استمراريتها. فاستراتيجية التوعية السيبرانية في شق لها تخضع إلى السرية وفي شق آخر تتطلب الشفافية والشرح والمشاركة وهذا جوهر الاختلاف بينها وبين باقي الاستراتيجيات الأخرى، حيث يشترط في نجاحها عدم معرفة الطرف الثاني (العدو) أو المنافس بوجهة نظر المؤسسة أو طريقة تعاملها مع المعلومات الرقمية، سواء كان هذا الطرف داخليا أو خارجيا.

Sur : mvet.gov.dz/المجال-الأم/consulte : 03/06/2024.

¹ عبد الرزاق محمد الدليمي، مرجع سابق، ص 45.

² بلقاسم بن روان، وسائل الإعلام والمجتمع، دراسة في الأبعاد الاجتماعية والمؤسسية، ط1، دار الخلدونية للنشر والتوزيع، القبة القديمة، الجزائر، 2007، ص21.

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر

مقاربة وصفية تحليلية

لهذا يتطلب إعداد استراتيجية التوعية السيبرانية في سرية وحفظها في سرية أيضا مع تصنيف المعلومات السرية من غيرها وتميز بين الأشخاص الذين يملكون الصلاحيات وبين ذوي الصلاحيات المحدودة، خلال كل مرحلة من مراحل التطوير أو التعديل أو التنفيذ والتدخل.

كما أن إعداد استراتيجية التوعية السيبرانية يتطلب خبرة وتجربة وكذا حنكة وفهما دقيقا من المؤسسات -خاصة الاستراتيجية منها- لمنحى التهديدات السيبرانية المتغير باستمرار وبسرعة حتى تستطيع تصميم برامج توعية سيبرانية مناسبة لمستخدميها وموجهة خصيصا لتحقيق أهداف مسطرة مسبقا، بالاعتماد على مختلف الوسائل والتقنيات سيما منها الاتصال الرقمي.

لهذا فإن استراتيجية التوعية السيبرانية لدى المؤسسات العمومية ليست معزولة ومنمذجة وفق نمط معين فحسب، بل هي متكاملة ومرنة تخضع تغييراتها وتعديلاتها إلى التعديلات والتغيرات التي تطرأ على محيط المؤسسة الداخلي والخارجي، مما يفرض تكيف استراتيجيات التوعية السيبرانية وفق هذه التغيرات.

تركز المؤسسة العمومية في استراتيجيتها للتوعية السيبرانية أساسا على ضمان اتصال رقمي فعال وهادف تلتزم فيه بإعداد وتنفيذ مخططاتها الرقمية كأهداف استراتيجية، كتحسين الوصول الرقمي للمستخدمين عن طريق توفير المحتويات الرقمية التي تفيدهم في التوعية السيبرانية وتطوير وتنويع المحتوى الرقمي، ما يضمن محتوى جذاب ومفيد عبر منصات تفاعلية متعددة ومواقع الواب ووسائل التواصل الاجتماعي ونشرات رسمية، ما يسمح بخلق بيئة تشجع على الاتصال وتبادل الأفكار والمعلومات.

كما يساهم الاتصال الرقمي بمختلف أدواته بإيصال المعلومات المتعلقة بالتهديدات السيبرانية والمخاطر المحتملة في وقتها مما يضمن الاستجابة السريعة واتخاذ الإجراءات اللازمة حين حدوثها، ويسمح أيضا باتخاذ إجراءات استباقية ووقائية عن طريق التوجيهات والإرشادات التي يستفيد منها الجمهور الداخلي على شكل دليل إرشادي أو مراسلات رسمية عن طريق الشبكة الداخلية أو عن طريق البريد الإلكتروني أو النشرات الإخبارية الداخلية أو فيديوهات تحسيسية تنشر داخل المؤسسات العمومية عبر شاشات العرض الإلكترونية، مما يساهم في تعزيز الفهم الجماعي للمخاطر والتهديدات السيبرانية المحتملة ويعزز بذلك التعاون بين المستخدمين في مواجهتها من جهة، وجعل المستخدم أكثر قدرة على التعرف على السلوكيات المشبوهة والممارسات غير الآمنة من جهة أخرى ويصبح بذلك كل مستخدم في مؤسسته سفيرا للأمن السيبراني.

تأسيسا لما سبق ذكره، ينبغي أن تتضمن استراتيجية التوعية السيبرانية في المؤسسة العمومية خطة عمل لتعزيز بيئة آمنة للمستخدمين وترسي مجموعة من القواعد والأهداف التي تسعى لتعزيز ثقافة الأمن السيبراني، بما في ذلك تأمين الجمهور الداخلي وحمايته وحماية مجهوده الفكري من التهديدات مع اتخاذ الإجراءات الاستباقية لمواجهة التهديدات المحتملة والتعافي منها بسرعة في حالة وقوعها، حيث يلعب الاتصال الرقمي دورا هاما في هذه الاستراتيجية من خلال:

- ✓ المساهمة في التوعية والتدريب وتوجيه المستخدمين لفهم كيفية حماية المعلومة من التهديدات السيبرانية وتحديات العالم الافتراضي من خلال تقديم دورات تدريبية وتكوينية حول كيفية التعامل مع البريد الإلكتروني ونهج السلوك السوي على الخط مع اعتماد أفضل الممارسات.
- ✓ التحقق من هوية الموظفين أثناء ولوجهم إلى مواقع واب أو المنصات الرقمية للمؤسسات بهدف ضمان تأمين بيئة العمل الافتراضية.
- ✓ التفاعل والردشة حول التهديدات، مع المستخدمين للإبلاغ عن أي نشاط مشبوه على الخط، أو أي هجمة سيبرانية.
- ✓ الردع السيبراني، يمكن الاتصال الرقمي من التصدي للهجمات وتنسيق التعاون والخبرات المؤسسة ومستخدميها للسيطرة على الهجمات وردعها في الحين لضمان بيئة عمل رقمية آمنة.
- ✓ المساهمة في تعزيز الثقافة السيبرانية لدى المستخدمين مما يجعلهم في حالة استنفار قصوى لمراقبة الأنشطة المشبوهة في صفحات واب المؤسسة باعتبارها من بين دعائم الاتصال الرقمية.
- ✓ بناء الوعي السيبراني للجمهور الداخلي على مستوى المؤسسة وهذا بدوره يساهم في رفع الوعي السيبراني على المستوى الوطني.

خاتمة:

يعدّ الاتصال الرقمي أداة رئيسية في نشر التوعية السيبرانية لدى المستخدمين (الجمهور الداخلي) للمؤسسة العمومية عن طريق نشر الوعي وتعزيز الثقافة السيبرانية أو بنائها في حالة انعدامها مع ضمان تدريبهم وتأهيلهم وبناء قدراتهم في مجال الأمن السيبراني الذي أضحت أولوية استراتيجية للمؤسسات والدول.

كما يساهم الاتصال الرقمي في تحسيس الجمهور الداخلي من المستخدمين بالتهديدات السيبرانية ومخاطرها عن طريق إشراكهم في الحملات التحسيسية والتفاعل الإيجابي ومرافقتهم في صناعة القرار ما يكسبهم الثقة وبالتالي الولاء للمؤسسة والدفاع عنها وعن مصالحها الرقمية في الفضاء السيبراني المفتوح على كل التهديدات المحتملة.

فنجاح استراتيجية التوعية السيبرانية في أي مؤسسة تفرض الهندسة الجيدة لها، التبني الجيد من قبل الجمهور الداخلي المؤهل لمجابهة مختلف التهديدات والقادر على التعافي بسرعة وبأقل الأضرار مع اعتماد أفضل الممارسات.

التوصيات:

- ✓ على المؤسسات العمومية التركيز أكثر على التوعية السيبرانية وإعطائها أهمية أكبر، مع المزج بين أساليب التوعية التقليدية ودعمها بالتوعية عبر الخط.

دور الاتصال الرقمي في تعزيز استراتيجية التوعية السيبرانية لدى الجمهور الداخلي للمؤسسة العمومية بالجزائر

مقاربة وصفية تحليلية

- ✓ على المؤسسات العمومية تنويع المحتوى التوعوي وجعله أكثر ديناميكية وجودة وتبسيط الرسائل التوعوية حتى تكون مفهومة وواضحة بالنسبة لجميع المستخدمين، أي التركيز على المضمون والشكل والهدف المراد تحقيقه بدقة.
- ✓ إعداد استراتيجيات توعية سيبرانية طويلة المدى مع قابلية القياس والتعديل وفق المستجدات وضمان المتابعة من قبل الإدارة العليا للمؤسسات العمومية.
- ✓ محاولة تخطي ذهنية التوعية من أجل رمي المسؤولية على المستخدم، بل التركيز على التوعية من أجل رفع الوعي والتأثير الإيجابي على السلوك السيبراني للمستخدمين الداخليين وتحفيزهم لتبني الأفكار التوعوية عبر أساليب الترغيب.
- ✓ التركيز بدرجة كبيرة على التكوين المستمر عبر الخط مع دعمه ببرامج وورشات تدريبية يشارك فيها الجميع والتوعية بأهمية المشاركة الفعالية فيها في أوساط المستخدمين الداخليين للمؤسسات العمومية.
- ✓ إعداد وتنفيذ سيناريوهات تمثيلية لهجمات سيبرانية، مع ضمان مشاركة الجميع في العملية، مع تكريم المتفوقين والمتحصنين من الهجمات المفتعلة وتشجيع الفئات الأخرى من أجل الاجتهاد أكثر للرفع من الوعي واليقظة لديهم.
- ✓ تعزيز اللحمة بين المستخدمين بالمؤسسات العمومية ودعم الثقة بينهم من أجل تكاتف الجهود للدفاع عن مصالح المؤسسة بما فيها التحصن من الهجمات السيبرانية.
- ✓ التعاقد مع الجامعات ومعاهد التكوين من أجل دعم قدرات المستخدمين في مجال الإعلام الآلي والأمن السيبراني مع ضمان تأطيرهم لمعرفة المستجدات الحاصلة في عالم القرصنة الالكترونية وأساليب الهجمات السيبرانية.
- ✓ الاهتمام أكثر بالاتصال وتثمينه أكثر والرفع من الميزانيات المخصصة له بما في ذلك الاتصال الرقمي، لأن الاتصال مازال محتقر نوعا ما في المؤسسات العمومية لأن ثماره ونتائجه لا ترى من قبل بعض المدراء والكف عن التسويق أكثر لنشاطات المدراء وصورهم أكثر عبر المحتوى الرقمي أي إعطاء حيز أكبر للمحتوى التوعوي السيبراني في عملية الاتصال المؤسسي وبالأخص عبر الوسائط الجديدة.
- ✓ التعاون بين المؤسسات العمومية فيما بينها وبين الخواص من أجل الاستفادة من الخبرات وإيجاد نموذج توعية سيبرانية أكثر ملائمة حول التهديدات السيبرانية وفعال وصالح لكل المؤسسات، يخص فئات المستخدمين كل حسب مستواه ووعيه، أي بناء نموذج وطني يخصص خطط رفع الوعي السيبراني بالمؤسسات العمومية خلال مدة محددة على سبيل المثال كل خمس سنوات.
- ✓ تشجيع الباحثين من جامعين ومستخدمين في المؤسسات العمومية على البحث ومواصلة البحث في آليات وسبل الحماية السيبرانية وتعزيز الأمن السيبراني بالمؤسسات مع دعمهم المادي والمعنوي وإعطائهم الأولوية في سياسات

التوظيف بالمؤسسات العمومية و التصنيف الوظيفي في الرتبة على نحو يليق بشهادتهم التخصصية و بقدراتهم العملية.

قائمة المراجع:

1. الكتب:

بلقاسم بن روان، وسائل الإعلام والمجتمع، دراسة في الأبعاد الاجتماعية والمؤسسية، ط1، دار الخلدونية للنشر والتوزيع، القبة القديمة، الجزائر، سنة 2007.

راشد حمد النعيمي، العولمة الإعلامية والسياسات الأمنية، الدار العربية للعلوم ناشرون، ط1، بيروت، لبنان، سنة 2020.
عبد الرزاق محمد الدليمي، المدخل إلى العلاقات العامة، دار الثقافة للنشر والتوزيع، ط1، المملكة الأردنية الهاشمية، سنة 2011.

فارس محمد العمارات، الأمن السيبراني، المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، الأردن، سنة 2022.
محمد عبد المجيد، نظريات الإعلام واتجاهات التأثير، عالم الكتاب، ط3، القاهرة، مصر، سنة 2004.
مي، العبد الله وآخرين، استراتيجيات الإعلام والاتصال في الحوب الراهنة؛ من الحرب الناعمة إلى المواجهة العسكرية، الجامعة اللبنانية، لبنان، 2022.

2. أطروحات دكتوراه ورسالة ماجستير:

صليحة، كاريش، دور أنظمة المعلومات في تنمية القدرة التنافسية للمؤسسة: حالة المؤسسة الجزائرية، رسالة ماجستير، كلية العلوم الاقتصادية، الجزائر، سنة 2000.

3. المؤتمرات والملتقيات والأيام الدراسية:

نسيسة أرحاب، الملتقى الوطني حول تعزيز القدرات في مجال الأمن السيبراني، النادي الوطني للجيش، 2022/02/10، الجزائر العاصمة.

Sur : mvvet.gov.dz : 03/06/2024. //ملتقى-وطني-لتعزيز-القدرات-في-مجال-الأمن

4. مواقع إلكترونية:

التحرير، كاسبريسكي: احباط أكثر من 13 مليون محاولة تصيد احتيالي في الجزائر خلال 2024، دزد شاركتي، 22مارس 2025. Sur : dzcharikati.net

زولا سومر، استهداف الجزائر بـ 70مليون هجمة سيبرانية خلال 10 أشهر، يومية المساء، الجزائر، 2024/11/18.
Sur : www.el-massa.com

علاء الدين حميدي، الأمن السيبراني: خط الدفاع الأول في العصر الرقمي، 2025/12/10،

الأمن-السيبراني-خط-الدفاع-الأول-في/2025/12/10/blogs/ Sur : www.aljazeera.net

لمياء حرزلاوي، 70 مليون هجمة إلكترونية في الجزائر خلال 2024، جريدة الفجر، 2024/11/17 : Sur .
alfadjer.dz/article/70-mlyon-hag-alktrony-fy-algzayr-khal-2024
consulté : <https://www.mpt.gov.dz/l-/15/O6/2025>.

محمد بلقور، الجزائر في معركة القرن: الأمن السيبراني كجبهة جديدة لحماية الدولة الوطنية، موقع الجزائر الآن،
2025/10/12.

Sur : algeriemaintenant.dz/2025/10/ الجزائر-في-معركة-القرن-الأمن-السيبراني /

مصطفى جالي، الأمن السيبراني في أفريقيا بين التحديات والرهانات الاستراتيجية، ورقة تحليلية، مركز الجزيرة للدراسات،
20 يوليو 2024، Sur: studies.aljazeera.net.

Metacompliance.cyber security awarness and the healthcare. Sur :
<https://www.metcompliance.com/blog/cyber-security-awarness>. Consulté :
12/04/2025.

https://www.ens-lagh.dz/16_05_2025/ consulté : 13/09/2025.

consulté : <https://www.mpt.gov.dz/l-/15/O6/2025> اطلاق-حملة-تحسيسية-وتوعوية-وطنية-حول-