

دور الاتصال في تعزيز الأمن السيبراني للمنظمات

The role of communication in enhancing the cyber security of organizations

بن توتة بشيرة

جامعة الجزائر 2 (الجزائر)، bachira.bentouta@univ-alger2.dz

تاريخ النشر: 2025 / 01 / 20

تاريخ القبول: 2025 / 01 / 10

تاريخ الاستلام: 2024 / 10 / 19

ملخص:

أصبح الاعتماد على الفضاء الرقمي جزءا أساسيا من حياتنا اليومية، مما زاد من الحاجة إلى فهم العلاقة بين السلوك السيبراني للأفراد وأمن البيانات، فقد يفتقر الأفراد إلى المعرفة الكافية حول ممارسات الأمن السيبراني وقد لا يدركون المخاطر التي تترتب على سلوكياتهم الرقمية، مثل مشاركة المعلومات الشخصية بشكل غير آمن أو استخدام كلمات مرور ضعيفة. هذه السلوكيات تعرض البيانات الحساسة للاختراق والتهديدات السيبرانية، وعليه نهدف من خلال هذه الورقة البحثية إلى تسليط الضوء على كيفية تأثير قنوات الاتصال المختلفة في تشكل الوعي بالمخاطر السيبرانية لدى الأفراد، وكيف يؤثر هذا الوعي على سلوكهم السيبراني في الفضاء الرقمي، إلى جانب التعرف على مدى التزامهم بالسياسات والإجراءات الأمنية المحددة داخل المنظمة.

الكلمات المفتاحية: الاتصال الفعال، الأمن السيبراني، السلوك السيبراني، أسلوب القيادة، الثقافة التنظيمية.

Abstract:

Reliance on the digital space has become an essential part of our daily lives, which has increased the need to understand the relationship between individuals' cyber behavior and data security, as individuals may lack sufficient knowledge about cyber security practices and may not be aware of the risks that their digital behaviors entail, such as sharing personal information insecurely or using weak passwords. These behaviors expose sensitive data to hacking and cyber threats. Therefore, we aim through this research paper to shed light on how different communication channels influence the formation of awareness of cyber risks among individuals, and how this awareness affects their cyber behavior in the digital space, in addition to identifying the extent of their compliance with the security policies and procedures defined within the organization.

Keywords: Cyber security , Cyber behavior. Driving style, Effective communication, Organizational culture.

1. مقدمة

في عصر التحول الرقمي المتسارع، أصبحت المنظمات تواجه تحديات كبيرة في الحفاظ على أمن بياناتها على الرغم من وجود تقنيات وأدوات متطورة لحماية المعلومات، حيث أصبح يتطلب هذا التحول حماية فعالة للمعلومات والبيانات، ومع هذه الفرص الجديدة، تأتي أيضا تحديات متعددة التي تتطلب وعيا دائما من قبل الموظفين، كزيادة الهجمات السيبرانية تعقيدا والتصيد الاحتيالي، البرمجيات الخبيثة، وهجمات الفدية، وقد يفتقر الأفراد إلى المعرفة الكافية حول ممارسات الأمن السيبراني، مما يجعلهم عرضة للاختراقات ويزيد من صعوبة تكيف المنظمات.

وقد أصبح الاعتماد على الفضاء الرقمي جزءا أساسيا من حياتنا اليومية، مما زاد الحاجة إلى فهم العلاقة بين السلوك السيبراني للأفراد وأمن البيانات، فقد يفتقر الأفراد إلى المعرفة الكافية حول ممارسات الأمن السيبراني وقد لا يدركون المخاطر التي تترتب على سلوكياتهم الرقمية، مثل مشاركة المعلومات الشخصية بشكل غير آمن أو استخدام كلمات مرور ضعيفة. هذه السلوكيات تعرض البيانات الحساسة للاختراق والتهديدات السيبرانية، علاوة على ذلك، يسهم نقص الوعي والتثقيف في مجال الأمن السيبراني في تفاقم هذه المشكلة. فبينما تتطور أساليب الهجوم السيبراني بشكل مستمر، يظل الأفراد في الغالب غير مجهزين بالمعرفة الكافية لحماية أنفسهم وبياناتهم. مما يؤدي إلى دائرة مفرغة من الثقة الزائدة والسلوكيات غير المسؤولة، مما ينعكس سلبا على الأمان العام للبيانات.

ومع تزايد التهديدات السيبرانية في هذا العالم متسارع رقمية، فرض تحديات جديدة على المنظمات لحماية معلوماتها ومواردها، ووجب عليها وضع استراتيجيات للتصدي للتهديدات والاختراقات المحتملة في فضاءها الرقمي، ومن أهم هذه الاستراتيجيات إرساء نظام اتصال فعال يعزز الوعي بالمخاطر ويشجع الموظفين على اتباع الممارسات الأمنية السليمة، مما يقلل من احتمالية حدوث الخروقات، لكن من جهة أخرى، قد يؤدي ضعف التواصل أو غياب سياسات واضحة إلى تفشي سلوكيات غير آمنة بين الموظفين، مما يزيد من تعرض المنظمة للمخاطر، كما أن وجود ثقافة اتصال مفتوحة قد يسهم في تعزيز سرعة الاستجابة للحوادث السيبرانية، بينما يمكن أن تؤدي الأحاديث غير الرسمية أو المعلومات المغلوطة إلى تفاقم الأزمات، وعليه نطرح التساؤل الرئيسي التالي:

كيف تساهم قنوات الاتصال المختلفة في تشكيل الوعي بالمخاطر السيبرانية لدى الأفراد؟ وكيف يؤثر هذا الوعي على سلوكهم السيبراني في الفضاء الرقمي؟
ويتفرع عنه الأسئلة الفرعية التالية:

- . ما دور الاتصال في تعزيز ثقافة الأمن السيبراني داخل المنظمة؟
- . كيف يمكن أن تساهم تقنيات الاتصال الحديثة في تعزيز الأمن السيبراني؟
- . ما دور القيادة في تعزيز الاتصال الفعال كجزء من استراتيجيات الأمن السيبراني؟

أولاً: مفهوم الاتصال

1. تعريف الاتصال:

يعرف الاتصال بأنه " عملية نقل وتبادل المعلومات الخاصة بالمؤسسة داخلها وخارجها، وهو وسيلة تبادل الأفكار والاتجاهات والرغبات بين أعضاء المؤسسة، مما يساعد على التماسك والترابط فيحقق رؤساء العمل ومعاونوهم التأثير المرغوب في تحريك الجماعة نحو الهدف، وهو أداة هامة لإحداث التغيير في السلوك البشري" (جبلي، 2003)

فالالاتصال عملية تخلق العلاقات الإنسانية عن طريق نقل المعارف والتجارب من أجل التأثير في الآخرين بتوجيههم وتغيير سلوكهم حسب الفهم المشترك الذي يوصلون له ولهذا تعتبر عملية الاتصال أساس التفاعل الاجتماعي، ويعتبر الاتصال هو سلطة، حيث تعد هذه الأخيرة عنصراً أساسياً في لتنظيم وهي تنطوي على جانبين جانب ذاتي وجانب موضوعي.

الجانب الذاتي: يعبر عن قبول الاتصال باعتباره سلطة.

الجانب الموضوعي: يشير إلى طابع الاتصال الذي بفضلها تكون السلطة مقبولة

2. عناصر الاتصال:

تتضمن عملية الاتصال مجموعة العناصر، أجمع أغلب العلماء عليها وهي: المرسل، المستقبل، القناة، الرسالة، وبفهم هذه المكونات تتحقق فاعلية الاتصال.

1.2 المرسل:

ويسمى المصدر أو المتصل أو المنبع، وهو شخص أو مجموعة من الأشخاص أو الهيئة أو الجهاز الذي يود أن يؤثر في الآخرين بشكل معين ليشاركه في الأفكار أو الاتجاهات أو خبرات معينة. (العمرى، 1986)

فالمرسل هو الطرف الأول من طرفي الاتصال الذي يوضح رسالته بكل الطرق الممكنة إما شفويا أو بوسيلة يختارها، فقد صاحب سلطة أو مسؤولاً في المؤسسة، يبلغ أموراً معينة لمؤوسيه أو العكس أن يكون المتصل هو المرؤوس الذي يريد تقديم اقتراح معين لرئيسه.

ويمكن القول إن المرسل هو كل من يبعث بمجموعة من التعليمات قصد إثارة سلوك محدد لدى الطرف الأخر، فالالاتصال كعملية تنظيمية تستند إلى فاعلين لهم من القدرة على التأثير في سلوك الطرف الآخر

2.2 الرسالة:

هي مجموعة المعاني التي يرسلها المصدر (المتصل)، فهي محتوى الاتصال لأنها المضمون المطلوب نقله أو توصيله مهما كان نوعه (معلومة، تقرير، شكوى)، لهذا تعرف بأنها الأفكار أو الحقائق لها غايات مقصودة وموجهة لها دلالات ومعاني يرغب المصدر إفادتها للمستقبل.

وتتنوع وتختلف الرسائل باختلاف تنوع الاتصالات، فنجد أن الرسائل الإدارية تركز على معلومات موضوعية فنية وقانونية مثل الرئيس الذي يحرص على نشر اللوائح والنصوص التنظيمية التي تجدد إجراءات العمل.

وقد تكون الرسالة وجيزة ومختصرة أو تأخذ عدة مظاهر وأشكال كرسالة شفوية أو إرشاد تعبيرية وتوجيهي أو على شكل كتابي.

3.2 المستقبل:

هو الطرف الثاني الأساسي في العملية الاتصالية، فيقوم بتفسير ما تلقاه من المرسل حسب خبرته السابقة، كما أنه يمثل الهدف المقصود من العملية الاتصالية، هذه الأخيرة تبدأ بالمرسل وتنتهي بالمستقبل الذي تصله الرسالة عبر قناة محددة، والمستقبل هو الفرد أو الجماعة التي تتلقى الأوامر والمعلومات والاقتراحات من

الطرف الآخر قصد التأثير والاشتراك، فلا بد ان تتحقق فعالية العملية الاتصالية والذي هدفها مشاركة الأفكار والمعلومات.

4.2 التغذية العكسية:

ونقصد بها الرسالة التي يبعثها المستقبل ردا على رسالة المصدر ليتحقق ركن المشاركة ومدى تحقيق الفهم المتبادل وهذا عن طريق استعمال الأساليب اللفظية أو الكتابية أو الرمزية، وهو رد المستقبل على ما تم استقباله ومدون في نص الرسالة.

5.2 القناة (وسيلة الاتصال):

لنقل الرسالة يجب استخدام وسيلة لربط المصدر مع المستقبل حتى تتحقق العملية الاتصالية، وتتم عن طريق توظيف قناة أو وسيلة لنقل المعلومات وتوصيلها إلى المستقبل، وقد تكون قولاً أو كتابة أو غيرها. وتتعدد أشكالها من وسائل وقنوات لفظية حيث تنقل المعاني والمعلومات عن طريق الرموز الصوتية مباشرة، وقد تكون كتابية ككتابة التقارير والتعليمات، ويمكن استعمال القنوات التقنية كالهاتف والانترنت وشبكات التواصل الاجتماعي.

3. قنوات الاتصال:

تندفق المعلومات داخل المؤسسة من خلال مجموعة من القنوات ونلخصها في الأشكال التالية:

الاتصال العمودي، والاتصال الأفقي، والاتصال النجمي.

3.1 الاتصال العمودي: ويضم نوعين من الاتصالات:

- الاتصال الهابط أو النازل: ويكون اتجاهه من الأعلى إلى الأسفل، ويكون من مستويات الإدارة العليا إلى المستويات التنفيذية، وفي هذا النوع من الاتصال يتم اتصال الرئيس بالمرؤوس بشكل رسمي وهو أكثر استخداماً في المنظمة، ويضم التوجيهات والإرشادات المتعلقة بإجراءات العمل التنظيمية والإدارية والفنية، ومن بين الوسائل التي يعتمد عليها هذا النوع من الاتصال الاجتماعات الرسمية والإعلانات المختلفة والنشرات الدورية.

- الاتصال الصاعد: وهو عكس الاتصال النازل، ينتقل من الأسفل إلى الأعلى ويخص الشكاوى والتقارير والطلبات المشاكل الشخصية المختلفة للعمال، أو استفسارات حول أداء العمل أو بعض النقاط الغامضة، ومن بين الوسائل المستعملة في هذا الاتصال كاجتماعات، علية الأفكار. (بوثلجة، 1996)

3.2 الاتصال الأفقي: تكون في نفس المستوى الإداري وتحدث عادة بين العمال، تضم الاتصالات التي تحدث بين الإطارات ومسؤولي المصالح فيما بينهم أي يكون بين فئات ذات خصائص سوسيو مهنية متشابهة، ويعتبر هذا النوع من الاتصال من أهم أنواع الاتصالات في المؤسسة نظراً لدوره الفعال في اختصار الوقت، حيث يهدف إلى ضمان التكامل بين المصالح والتنسيق بينها لتحقيق الغايات المسطرة.

3.3 الاتصال النجمي: سمي كذلك لكثرة تعقيده وتشابكه إذ يشبه النجمة لكثرة اتجاهاته، ويميز التنظيمات الحديثة التي تميل وتتجه نحو التعقيد ويشمل الاتصالات العمودية بنوعها الصاعد والنازل والاتصالات الأفقية، وتعتبر من الاتصالات الأكثر فعالية في مؤسسة اليوم.

4. الاتصالات الرسمية وغير رسمية:

يوجد تصنيف آخر لأنواع الاتصالات من حيث طبيعتها سواء كانت رسمية أو غير رسمية. الاتصالات الرسمية: هي تلك الصادرة من النصوص التنظيمية واللوائح والمنشورات وهي تصدر عن السلطة الرسمية.

. الاتصالات غير رسمية: وهي تأتي بشكل غير مقنن وبطرق غير مضبوطة وتكون خارج نطاق السلطة، وتصدر عن مصادر التنظيم غير رسمي ومن بين وسائلها العلاقات الاجتماعية كفي حالة تقديم شكوى أو خطاب شفوي.

5. طرق عملية الاتصال:

تعددت الطرق لنقل المعلومات وإيصالها نذكر منها:

1.5 الاتصال الكتابي: ويعتبر الأسلوب الكتابي الأكثر تداولاً في المؤسسة لالتسامه بالطابع الرسمي والديمومة، حيث يمكن الاحتفاظ بالرسائل الكتابية والعودة إليها عند الضرورة والحاجة، ونظراً لتعدد المهام وكثرة الرسائل والمعلومات المنقولة فيصعب استيعابه بطرق أخرى فتبقى الوسيلة الأكثر نجاعة للاسترشاد بها كل ما استدعت الحاجة إليها.

2.5 الاتصال الشفوي: تكون اما شفويا مباشرة وجها لوجه أو المحادثات المختلفة، ومن بين مزاياها تقدم معلومات آنية مباشرة.

3.5 الاتصال غير اللفظي: تكون عن طريق التعبير والإيماءات المختلفة للوجه أو حركات الجسد فهذا يعطي دلالات عن الرضا أو عدم الموافقة.

ثانياً: مفهوم الأمن السيبراني:

1. تعريف الأمن السيبراني:

يشير مفهوم الأمن السيبراني إلى مجموعة من التدابير والعمليات والتقنيات المصممة لحماية الأنظمة والشبكات والمعلومات من الهجمات والتخريب. ويشمل ذلك مجموعة واسعة من الأنشطة التي تهدف إلى الحفاظ على سرية وسلامة وموثوقية البيانات في الفضاء السيبراني. (طارق، 2021)

2.1 أهداف الأمن السيبراني:

. حماية البيانات: التأكد من أن البيانات المخزنة أو المنقولة تظل سرية وسليمة.
. إدارة المخاطر: تقييم المخاطر المحتملة وتطوير استراتيجيات للتخفيف منها.
. التحكم في الوصول: استخدام تقنيات مثل المصادقة والتشفير لضمان وصول الأشخاص المصرح لهم فقط إلى المعلومات الحساسة.

. الاستجابة للحوادث: وضع خطط للاستجابة السريعة والفعالة عند حدوث أي خرق أمني.
. التوعية والتدريب: رفع مستوى الوعي بين الأفراد بشأن التهديدات السيبرانية وكيفية التصرف بحذر.
. الامتثال: الالتزام بالمعايير والقوانين المتعلقة بحماية البيانات، مثل اللائحة العامة لحماية البيانات. (السلام، 2022)

3.1 عناصر الأمن السيبراني:

. التحكم في الوصول: تنظيم من يمكنه الوصول إلى المعلومات والأنظمة، سواء من خلال كلمات المرور، أو المصادقة متعددة العوامل.
. التشفير: حماية البيانات من خلال تحويلها إلى صيغة غير قابلة للقراءة إلا للأشخاص المصرح لهم، مما يحمي المعلومات الحساسة أثناء النقل والتخزين.
. جدران الحماية (Firewall): تعمل على مراقبة وتصفية حركة البيانات بين الشبكات، ومنع الوصول غير المصرح به.
. برامج مكافحة الفيروسات: تستخدم للكشف عن البرامج الضارة وإزالتها، وحماية الأنظمة من التهديدات المعروفة والجديدة.

- التحديثات الأمنية :تطبيق تحديثات منتظمة للبرامج والأنظمة لضمان تصحيح الثغرات الأمنية التي قد تستغلها الهجمات.

- التدريب والتوعية :تعزيز الوعي بين الموظفين حول المخاطر السيبرانية وأفضل الممارسات لحماية المعلومات.

- إدارة المخاطر :تحديد وتقييم المخاطر المحتملة ووضع استراتيجيات للتخفيف منها.

- النسخ الاحتياطي للبيانات :إنشاء نسخ احتياطية منتظمة للبيانات لضمان استعادتها في حالة فقدانها أو تعرضها لهجوم.

- المراقبة والتحليل :استخدام أدوات لرصد الشبكة وتحليل الأنشطة المشبوهة للكشف عن التهديدات في وقت مبكر.

- استجابة الحوادث :وضع خطط وإجراءات للتعامل مع الحوادث الأمنية عند حدوثها، لضمان استجابة سريعة وفعالة. (فوزي، 2016)

2. مفهوم السلوك السيبراني:

1.2 تعريف السلوك السيبراني:

السلوك السيبراني يشير إلى الأفعال والتصرفات التي يقوم بها الأفراد عند استخدامهم للتكنولوجيا، خاصة في الفضاء السيبراني. يشمل ذلك كيفية تفاعل الأفراد مع المعلومات، الأنظمة، والبيانات على الإنترنت، فضلا عن استجاباتهم للتهديدات والمخاطر، ففهم السلوك السيبراني يمكن أن يساعد المؤسسات في تعزيز الأمن السيبراني من خلال تطوير استراتيجيات تستهدف تعزيز السلوكيات الإيجابية وتقليل السلوكيات الضارة. ونقصد بالأمن السيبراني بالكيفية التي يتفاعل بها الافراد مع التكنولوجيا وكيفية استخدامهم للأجهزة والبرامج في بيئات العمل، وكيفية استجابتهم للمواقف والمخاطر السيبرانية، مثل الهجمات الإلكترونية أو محاولات التصيد، إلى جانب مدى التزامهم بالسياسات والإجراءات الأمنية المتبعة في المنظمة، والأنماط السلوكية المتكررة، مثل إدارة كلمات المرور، مشاركة المعلومات، أو التعامل مع البيانات الحساسة، ومستوى الوعي بالمعرفة بالمخاطر المتعلقة بالفضاء السيبراني وكيفية الوقاية منها.

2.2 محددات السلوك السيبراني:

- الوعي بمخاطر البيئة الرقمية: يقصد به وعي الأفراد بالمخاطر السيبرانية، مثل التصيد الاحتيالي والبرمجيات الخبيثة، ويؤثر على كيفية تصرفهم في الفضاء الرقمي، كاستخدام كلمات مرور قوية وتحديثها بانتظام الذي يحمي المعلومات الحساسة، إلى جانب عدم فتح الروابط المشبوهة أو المرفقات غير المعروفة الذي قد يؤدي إلى الاختراقات، والالتزام بالسياسات والإجراءات الأمنية المحددة داخل المنظمة التي تقلل من المخاطر سرقة البيانات والاختراق. (محمد، 2013)

- المعارف السابقة: المعارف والمعلومات في مجال التكنولوجيا والأمن السيبراني تلعب دورا مهما في تحديد كيفية تصرف الأفراد.

- الثقافة التنظيمية :ثقافة المؤسسة وتأثيرها على سلوك الموظفين في التعامل مع التكنولوجيا وحماية المعلومات.

3.2 تحديات السلوك السيبراني:

هناك عدة تحديات مرتبطة بالسلوك السيبراني نذكر منها:

- الهجمات السيبرانية:تزايد الأساليب الهجومية، مثل التصيد الاحتيالي، يتطلب وعيا دائما من الأفراد.

- المسؤولية المشتركة: كل فرد داخل المنظمة يحمل مسؤولية الأمن السيبراني، مما يتطلب ثقافة مشتركة تعزز السلوكيات الآمنة.

4.2 استراتيجيات تعزيز السلوك السيبراني:

لتعزيز السلوك الإيجابي لدى الأفراد حتى يتصدون للهجمات والاختراقات الناتجة عن الثغرات المتعددة يجب على المنظمات اعداد خطط واستراتيجيات وقائية نذكر منها:

التدريب والتوعية :تنظيم ورش عمل ودورات تدريبية لتثقيف الموظفين حول أحدث التهديدات وأساليب الحماية.

.تحفيز الممارسات الجيدة: تقديم مكافآت أو اعترافات للموظفين الذين يظهرون سلوكيات أمنية جيدة.

. استخدام أدوات الأمن السيبراني :تطبيق برامج مضادة للفيروسات وجدران الحماية لمراقبة الأنشطة غير الطبيعية.

. تحليل البيانات: استخدام تقنيات تحليل البيانات لاكتشاف الأنماط السلبية في سلوك المستخدمين.

- تهيئة بيئة آمنة :تشجيع بيئة عمل تدعم الحوار المفتوح حول الأمن السيبراني، مما يسهل الإبلاغ عن الحوادث.

ثالثا: الاتصال وأثره في تعزيز الأمن السيبراني:

1. قنوات الاتصال ودورها في تشكّل الوعي بالمخاطر السيبرانية:

تلعب قنوات الاتصال دورا محوريا في تشكيل الوعي بالمخاطر السيبرانية، حيث تتيح تبادل ومشاركة المعلومات حول التهديدات السيبرانية، مما يساعد الأفراد على فهم المخاطر الحالية والمحتملة، فتوفر ورش العمل والدورات التدريبية عبر الإنترنت معلومات عن كيفية التعرف على المخاطر، مثل التصيد الاحتيالي والبرمجيات الخبيثة، ومن خلال قنوات الاتصال، يمكن إرسال تحديثات دورية حول أحدث التهديدات، مما يساعد الأفراد على البقاء على اطلاع، إلى جانب مشاركة والتجارب وتبادل قصص حقيقية عن حوادث سيبرانية تؤدي إلى تعزيز الوعي، حيث يتعلم الأفراد من تجارب الآخرين، كما تقدم قنوات الاتصال نصائح وإرشادات حول كيفية حماية المعلومات الشخصية واتباع الممارسات الأمنية، كما تساعد هذه القنوات في استطلاعات الرأي والتغذية الراجعة من خلال قياس مستوى الوعي بالمخاطر السيبرانية وتحديد المجالات التي تحتاج إلى مزيد من التثقيف.

ومن جهة أخرى تعمل قنوات الاتصال على خلق ثقافة أمان وشعور الأفراد بالمسؤولية تجاه حماية المعلومات والمشاركة في تعزيز الوعي، وتحفيز والتزام الأفراد بالممارسات الأمنية من خلال الحملات التوعوية والتواصل المستمر.

كما تساهم قنوات الاتصال في الاستجابة السريعة للمخاطر فتتيح تبادل المعلومات حول التهديدات الجديدة بسرعة، مما يساعد الأفراد على اتخاذ إجراءات وقائية، وتقديم موارد مثل الأدلة والنصائح حول كيفية التعامل مع المخاطر من خلال المواقع الإلكترونية والنشرات الإخبارية، إضافة إلى ذلك تساعد في توجيه النقاشات حول الأمن السيبراني داخل المنظمات، مما يعزز من فهم الموظفين للمسؤوليات الملقاة على عاتقهم، وتشجيع الأفراد على المشاركة في الأنشطة الأمنية، مثل اختبار الأمان أو المسابقات من خلال الحملات التوعوية، كما توفر قنوات الاتصال تقارير حول اتجاهات الهجمات السيبرانية يمكن أن يعزز من فهم الأفراد للتحديات الراهنة في مجال الأمن السيبراني، ويضمن استخدام أساليب وقنوات التواصل المتنوعة مثل الفيديوها، المقالات، والرسائل النصية وصول المعلومات لفئات مختلفة من الأفراد بطرق تناسبهم، وتساعد قنوات الاتصال في جمع البيانات حول الوعي بالمخاطر وتقديم تحليل مستمر لتحديد الثغرات في المعرفة، باستخدام هذه الأساليب، تساهم قنوات الاتصال في تعزيز الوعي بالمخاطر السيبرانية، مما يمكن الأفراد من اتخاذ قرارات أفضل لحماية أنفسهم ومعلوماتهم، فالارتباط الفعال يعزز شعور الانتماء والالتزام لدى الموظفين، مما يجعلهم أكثر حرصا على اتباع السياسات والإجراءات الأمنية.

2. دور الاتصال في تعزيز ثقافة الأمن السيبراني داخل المنظمة:

تعرف الثقافة التنظيمية على أنها مجموعة المبادئ الأساسية التي اخترعتها الجماعة أو اكتشفها وطورها أثناء حل مشكلاتها للتكيف الخارجي والاندماج الداخلي والتي أثبتت فاعليتها ومن ثم تعليمها للأعضاء الجدد كأحسن طريقة للشعور بالمشكلات وإدراكها وفهمها، وهي كذلك مجموعة من الافتراضات والاعتقادات والقيم والقواعد والمعايير التي تشترك بها أفراد المنظمة. وهي بمثابة البيئة الانسانية التي يؤدي الموظف عمله فيها. فهي موجودة بأي شكل من الأشكال ولا يمكن أن ترى مؤسسة بشى أنواعها خالية من هذا العنصر الحيوي الذي يرتبط بالدرجة الأولى بالأفراد المنتمين فيها إلى أي منظمة. (الحميان، 2019)

وتساهم الثقافة التنظيمية التي تركز على الاتصال المفتوح في ترسيخ قيم الأمن السيبراني وذلك عن طريق تعزيز الوعي المشترك بين جميع الموظفين حول أهمية الأمن السيبراني، مما يجعلها جزءاً من الهوية المؤسسية، ومن خلال تشجيع المشاركة الفعالة للموظفين للتعبير عن مخاوفهم أو اقتراحاتهم بشأن الأمن السيبراني، يشعرون بأنهم جزء من الجهود الأمنية، مما يعزز الالتزام بالقيم الأمنية، وتوفر الثقافة التي تركز على الاتصال فرصاً للتدريب المستمر، مما يضمن تحديث المعلومات والمهارات اللازمة للتعامل مع المخاطر السيبرانية، و القادة الذين يتبنون قيم الاتصال والأمان، فيصبحون قدوة يحتذى بها للموظفين، مما يعزز سلوكياتهم في مجال الأمن السيبراني، كما تسهل ثقافة الاتصال توفير الموارد اللازمة والتوجيه لدعم جهود الأمن السيبراني، مما يساعد في خلق بيئة آمنة، ويساعد الاتصال الفعال في توزيع المعلومات حول التهديدات والاتجاهات في الأمن السيبراني بشكل دوري، مما يعزز الوعي المستمر، كما تشجع الثقافة التي تركز على الاتصال على تبادل المعرفة والخبرات، مما يعزز التعلم المستمر حول الأمن السيبراني.

وكخلاصة تساهم الثقافة التنظيمية التي تركز على الاتصال في خلق بيئة يشعر فيها الموظفون بالأمان عند الإبلاغ عن الحوادث أو المخاطر دون خوف من العقوبات، كما تعزز ثقافة الاتصال الفعال التعاون بين الفرق المختلفة لتحقيق أهداف الأمن السيبراني، وتساهم في ترسيخ قيم الأمن السيبراني من خلال تعزيز الوعي، المشاركة، التعلم، والدعم، مما يساعد في بناء بيئة عمل أكثر أماناً.

3. دور القيادة الفعالة في تعزيز الاتصال الفعال كجزء من استراتيجيات الأمن السيبراني:

تشير القيادة الفعالة إلى القدرة على توجيه الأفراد لتحقيق الأهداف المشتركة بكفاءة وتأثير من خلال القدرة على نقل الأفكار بوضوح والاستماع للآخرين ووضع أهداف محددة وملهمة تجعل الفريق يعمل نحو تحقيقها، كما يقوم القائد الفعال بتحفيز وتشجيع الأفراد ودعمهم لتحقيق إمكاناتهم الكاملة، ويتسم بالمرونة والقدرة على التكيف مع التغيرات والتحديات التي تواجه الفريق، والقدرة على تحمل المسؤولية عن القرارات والنتائج، سواء كانت إيجابية أو سلبية، إلى جانب القدرة على بناء الثقة وخلق بيئة آمنة تشجع على التعاون والابتكار. (سعاد، 2018)

ونقصد بالقائد الفعال هو ذلك القائد الذي يبرز أهمية الأمن السيبراني ويجعله جزءاً من ثقافة العمل ويمكن أن يحفز الأفراد على اتباع ممارسات آمنة، إلى جانب قدرته على التواصل الفعال ووضوح حول المخاطر والسياسات المتعلقة بالأمن السيبراني ويساهم في زيادة وعي الأفراد مما يعزز سلوكياتهم الإيجابية، كما يحرص التدريب المستمر والدعم الفني الذي يجعل الأفراد أكثر قدرة على التعرف على المخاطر والتعامل معها بشكل فعال، كما يستخدم الحوافز لتشجيع السلوكيات الآمنة التي تعزز الالتزام بالأمن السيبراني ويحفز الأفراد على اتخاذ الإجراءات الوقائية، وهو نموذج للقائد الذي يحتذى به، فالقيادة الفعالة تلعب دوراً حاسماً في تشكيل السلوك السيبراني وتعزيز الأمن في بيئة العمل.

القادة الذين يقدمون الدعم والتوجيه في مجال الأمن السيبراني يعززون من وعي الموظفين ويشجعونهم على اتخاذ إجراءات وقائية، كما أن القيادة الفعالة تعمل على تخصيص الموارد لتدريب الموظفين على ممارسات

الأمان، مما يزيد من وعيهم بالمخاطر وكيفية التعامل معها، إلى جانب أهمية فتح قنوات التواصل فالقادة الذين يشجعون على التواصل المفتوح حول القضايا الأمنية يمكنون الموظفين من الإبلاغ عن المخاطر أو الحوادث دون خوف من العقاب، كما أن القيادة القوية تساهم في بناء ثقافة تنظيمية تشجع على الالتزام بالأمان، مما يعزز من وعي الموظفين ويقلل من السلوكيات غير الآمنة، إلى جانب أهمية توفير موارد مرجعية وإنشاء مكتبة من الموارد، مثل كتيبات إرشادية أو فيديوهات تعليمية، يمكن للموظفين الرجوع إليها عند الحاجة، كما أن تعزيز المشاركة وتشجيع الموظفين على المشاركة في مجموعات النقاش أو اللجان المتعلقة بالأمن السيبراني يعزز الشعور بالمسؤولية، ومشاركة القصص الناجحة وحالات واقعية عن اختراقات أو حوادث تمت معالجتها بشكل فعال، مما يساعد الموظفين على فهم الأهمية العملية للأمان. والقيادة التي لا توفر التدريب المستمر والدعم الفني تجعل الأفراد أقل قدرة على التعرف على المخاطر والتعامل معها بشكل فعال، واستخدام الحوافز لتشجيع السلوكيات الآمنة يمكن أن يعزز الالتزام بالأمن السيبراني ويحفز الأفراد على اتخاذ إجراءات وقائية، ويشكلون القادة الذين يمارسون سلوكيات آمنة بأنفسهم نموذجاً يحتذى به، مما يعزز من احتمالية اتباع الآخرين لنفس السلوك. ونستخلص مما تم عرضه أن للاتصال تأثير كبير في تعزيز السلوك السيبراني، ويمكن تلخيص هذا التأثير من خلال:

- . التوعية والتعليم: يساعد الاتصال الفعال في نشر المعلومات حول المخاطر السيبرانية وطرق الحماية.
- . برامج التدريب وورش العمل تعزز من وعي الموظفين وتساعدهم على فهم أهمية الأمان السيبراني.
- تبادل المعلومات :يسهل الاتصال بين الفرق المختلفة داخل المنظمة تبادل المعلومات حول التهديدات والمخاطر، هذا التواصل يساعد في تعزيز استجابة سريعة وفعالة عند حدوث حوادث سيبرانية.
- يعزز الاتصال المفتوح والثقافة التنظيمية التي تركز على الأمان من مشاركة الموظفين في اتخاذ القرارات الأمنية والتعبير عن مخاوفهم، مما يساهم في تحسين السلوك السيبراني.
- الإبلاغ عن الحوادث: وجود قنوات اتصال واضحة للإبلاغ عن الحوادث السيبرانية يشجع الموظفين على الإبلاغ عن المشاكل بسرعة، مما يساعد في تقليل الأضرار المحتملة.
- الدعم والتوجيه: الاتصال الجيد يوفر الدعم والتوجيه للموظفين في كيفية التعامل مع التهديدات، مما يزيد من قدرتهم على اتخاذ قرارات سليمة في المواقف الصعبة.
- مراقبة الأداء :يساهم الاتصال في تقييم الأداء الأمني والتحسين المستمر من خلال تقديم التغذية الراجعة والملاحظات.
- فالاتصال الفعال والمتواصل يساهم في تعزيز سلوك الأفراد في الفضاء السيبراني، مما يؤدي إلى بيئة عمل أكثر أماناً وفاعلية.
- إن القيادة التي لا توفر التدريب المستمر والدعم الفني تجعل الأفراد أقل قدرة على التعرف على المخاطر والتعامل معها بشكل فعال، واستخدام الحوافز لتشجيع السلوكيات الآمنة يمكن أن يعزز الالتزام بالأمن السيبراني ويحفز الأفراد على اتخاذ إجراءات وقائية، ويشكلون القادة الذين يمارسون سلوكيات آمنة بأنفسهم نموذجاً يحتذى به، مما يعزز من احتمالية اتباع الآخرين لنفس السلوك.
- . كما أن للممارسات اليومية الواعية كاستخدام كلمات مرور قوية وتحديثها بانتظام يمكن أن يحمي المعلومات الحساسة، إلى جانب السلوك الإيجابي عند التعامل مع الروابط كعدم فتح الروابط المشبوهة أو المرفقات غير المعروفة التي يؤدي إلى الاختراقات، كما أن اتباع الإجراءات الالتزام بالسياسات المحددة داخل المنظمة يمكن أن يقلل من المخاطر.

- يعزز التواصل الفعال الوعي بمخاطر الفضاء الرقمي، فالقادة الذين يتواصلون بوضوح حول المخاطر والسياسات المتعلقة بالأمن السيبراني يساهمون في زيادة وعي الأفراد، مما يعزز سلوكياتهم الإيجابية.
- من الضروري أن تتبنى المؤسسات برامج تدريب شاملة وتخلق ثقافة تحفز الموظفين على الاهتمام بالأمن، إلى جانب توفير برامج دعم نفسي مثل الاستشارات يمكن أن يساهم في تخفيف الضغوط النفسية، وتنظيم ورش عمل تدريبية دورية لتعزيز الوعي الأمني، حتى في أوقات الضغط.
- أن زيادة الاعتماد على التكنولوجيا والأنظمة الرقمية قد يؤدي إلى إغفال بعض الموظفين لأهمية الممارسات التقليدية للأمان، كما أن التغييرات المفاجئة والتحولات السريعة في البيئة التكنولوجية أو تنظيم العمل كالمعمل عن بعد قد تؤدي إلى عدم استعداد الموظفين لمواجهة التحديات الأمنية الجديدة،
- أهمية توفير موارد مرجعية وإنشاء مكتبة من الموارد، مثل كتيبات إرشادية أو فيديوهات تعليمية، يمكن للموظفين الرجوع إليها عند الحاجة.
- تشجيع الموظفين على المشاركة في مجموعات النقاش أو اللجان المتعلقة بالأمن السيبراني يعزز الشعور بالمسؤولية، ومشاركة القصص الناجحة وحالات واقعية عن اختراقات أو حوادث تمت معالجتها بشكل فعال، مما يساعد الموظفين على فهم الأهمية العملية للأمان.
- الضغوط والتوتر في مكان العمل يمكن أن يكون لهما تأثيرات كبيرة على أداء الموظفين وسلوكهم، بما في ذلك سلوكياتهم المتعلقة بالأمن السيبراني. فهم هذه العلاقة يساعد المنظمات على تحسين بيئة العمل وتعزيز الأمن السيبراني، فالضغوط النفسية يمكن أن تؤدي إلى تشتت تركيز الموظفين، مما يزيد من احتمال حدوث أخطاء مثل فتح روابط مشبوهة أو إدخال معلومات حساسة بشكل غير صحيح، وقد يتسبب التوتر في تجاهل الموظفين للمعايير الأمنية، مثل عدم تحديث كلمات المرور أو عدم اتباع بروتوكولات الأمان.
- كما أن للممارسات اليومية الواعية كاستخدام كلمات مرور قوية وتحديثها بانتظام يمكن أن يحمي المعلومات الحساسة، إلى جانب السلوك الإيجابي عند التعامل مع الروابط كعدم فتح الروابط المشبوهة أو المرفقات غير المعروفة التي يؤدي إلى الاختراقات، كما أن اتباع الإجراءات الالتزام بالسياسات المحددة داخل المنظمة يمكن أن يقلل من المخاطر.
- تشجيع الموظفين على المشاركة في مجموعات النقاش أو اللجان المتعلقة بالأمن السيبراني يعزز الشعور بالمسؤولية، ومشاركة القصص الناجحة وحالات واقعية عن اختراقات أو حوادث تمت معالجتها بشكل فعال، مما يساعد الموظفين على فهم الأهمية العملية للأمان.

خاتمة:

يلعب السلوك السيبراني للأفراد داخل المنظمة يلعب دوراً محورياً في تعزيز أو إضعاف الأمن الرقمي. يتأثر هذا السلوك بعوامل عدة، منها الثقافة التنظيمية، مستوى الوعي، والتدريب المتاح. عندما يكون الموظفون مدركين للمخاطر السيبرانية ويتبعون ممارسات آمنة، فإنهم يساهمون في حماية المعلومات والبيانات الحساسة، مما يقلل من احتمالية وقوع الاختراقات والهجمات.

من جهة أخرى، فإن السلوكيات غير المسؤولة، مثل تجاهل السياسات الأمنية أو استخدام كلمات مرور ضعيفة، يمكن أن تفتح ثغرات خطيرة في النظام. لذا، من الضروري أن تعمل المنظمات على تعزيز ثقافة الأمان السيبراني من خلال التدريب المستمر، وتعزيز التواصل المفتوح حول المخاطر، وتوفير بيئة داعمة تشجع على الالتزام بالممارسات الأمنية.

ويعد الاتصال الفعال يعد حجر الزاوية في تعزيز الأمن السيبراني داخل المؤسسات. من خلال توفير قنوات تواصل مفتوحة ومستمرة، يمكن للمنظمات رفع مستوى الوعي بالمخاطر السيبرانية وتعزيز سلوكيات الأمان بين الموظفين. كما أن القيادة تلعب دوراً محورياً في ترسيخ ثقافة الأمان من خلال النموذج الإيجابي والتوجيه المستمر.

إن الاستثمار في استراتيجيات الاتصال الفعال لا يساهم فقط في حماية المعلومات والأنظمة، بل يعزز أيضاً من التعاون والتنسيق بين الفرق المختلفة، مما يخلق بيئة عمل أكثر أماناً وفعالية. في عالم يتطور بسرعة، حيث تتزايد التهديدات السيبرانية، يصبح الاتصال الفعال ضرورة وليس خياراً، مما يتطلب من جميع المؤسسات دمج هذا العنصر في استراتيجياتها الأمنية لضمان حماية شاملة وموثوقة.

في النهاية، يُعد وعي الأفراد وسلوكهم السيبراني خط الدفاع الأول ضد التهديدات الرقمية. لذلك، فإن الاستثمار في تطوير هذا الوعي هو استثمار في أمان المنظمة ككل.

قائمة المراجع:

- أبو النجا، محمد العمري. (1986). *الاتصال في الخدمة الاجتماعية*. الإسكندرية: دار المعرفة الجامعية.
- الحميان، م. م. س. (2019). *السلوك التنظيمي في منظمات الاعمال*. عمان: دار وائل للنشر.
- السلام، ح. ع. (2022). *التوعية بالأمن السيبراني: دليل الموظف*. القاهرة: مؤسسة الفكر العربي.
- سعاد، ف. (2018). *السلوك السيبراني: فهم المخاطر والتحديات*. القاهرة: دار العلوم.
- طارق، ا. (2021). *الأمن السيبراني: المفاهيم والتطبيقات العملية*. الاسكندرية: دار المناهج.
- علي عبد الرازق جبلي. (2003). *علم اجتماع التنظيم (مدخل للتراث والمشكلات والمنهج*. القاهرة: دار الشروق.
- غياث بوثلجة. (1996). *مقدمة في علم النفس التنظيمي*. الجزائر: ديوان المطبوعات الجامعية.
- فوزي، أ. (2016). *الأمن السيبراني دار الكتب العلمية*. الاسكندرية: دار المعارف.
- محمد، ز. (2013). *أمن الشبكات*. القاهرة: دار شمس للطباعة.