الجانب المظلم للتكنولوجيا

مخاطر العصر الرقمي تنتقص من مزاياه

كريس ويليش

لنا التكنولوجيا الرقمية سبلا عديدة من الراحة لم يكن الجيل السابق ليتخيلها. فالإنترنت **وفرت** يوفر على الطلبة والمتخصصين ساعات من البحث المرهق في المكتبات، ويتيح التواصل المرئي والشفهي والكتابي الفوري بدون أي تكلفة تُذكر. ويمكن لأي شخص يمتلك هاتف ذكي أن يستخدم نظام تحديد المواقع العالمي كي لا يفقد طريقه في مدينة غير معروفة له أو للعثور على أقرب فرع لمقهى ستاربكس. وتوجد خدمات تسوق وصيرفة للعملاء عبر الإنترنت، كما توجد أدوات يمكن للأطباء استخدامها في التشخيص باستخدام الكمبيوتر. وهذه هي عجائب العصر الرقمي الذي يصفه الخبيران إريك برينجولفسون وأندرو ماكافي باسم «العصر الآلي الثاني»، ليقروا بأن أجهزة الكمبيوتر توفر علينا المجهود العقلي كما وفرت علينا الماكينات البخارية المجهود العضلي.

ولكن لا يخلو هذا التقدم من أوجه قصور. فبعض نقاد العصر الرقمي يحزنهم سيطرة عدد قليل من وسائل التواصل الاجتماعي الضخمة على الرأي العام. ويثير البعض مخاوف مهمة إزاء الأمراض المقترنة بالعالم الرقمي، مثل رسائل التهديد الإلكترونية أو نشر المواد الإباحية عبر شبكة الإنترنت. وهناك البعض ممن يشعرون بالقلق حيال إمكانية اختراق خصوصيتهم والمخاطر التي تهدد الحريات المدنية في وقت تترك فيه كل حركة ومكالمة هاتفية ورسالة إلكترونية بصمة رقمية يمكن أن يستغلها جار فضولي أو حكومة قمعية.

وفي حين أن جميع هذه المخاوف مشروعة فمن المستحيل تحديد تكلفتها. ولكن توجد بعض جوانب التكنولوجيا الرقمية التي تفرض تكلفة ضخمة على الشركات والاقتصادات توازن جزءا على الأقل من الكفاءة التي يتيحها العصر الآلي الثاني.

فيمكن لقراصنة الإنترنت السيطرة على السيارات أو إغلاق شبكة كهرباء. ويسرق لصوص الإنترنت المعلومات الشخصية ويستخدمونها في الاستحواذ على الأموال المودعة في الحسابات المصرفية أو إجراء مشتريات احتيالية عبر الإنترنت باستخدام بطاقات ائتمان مملوكة لأشخاص آخرين. وبينما تمثل خدمات البريد الإلكتروني والهواتف المحمولة ووسائل التواصل الاجتماعي ثورة في عالم الاتصالات، فإنها تؤثر سلبا على إنتاجية الموظفين الذين يتابعون تحديثات تويتر لحظة بلحظة أو يدمنون استخدام تطبيقات الرسائل الفورية.

المخاطر الأمنية على شبكة الإنترنت

وعندما قررت مجموعة من الضباط السابقين في وحدة الاستخبارات الإلكترونية الإسرائيلية رقم ٨٢٠٠ إنشاء شركة خاصة في قطاع أمن تكنولوجيا المعلومات، اتفقوا على أن السيارات المتصلة بالإنترنت ستكون هي الابتكار الأهم على الإطلاق في المرحلة التالية.

ويقول يوني هيلبرون، نائب الرئيس لشؤون التسويق بشركة أرغوس سايبر سيكيوريتي المحدودة، «لقد عكفوا على مراقبة التطورات في الأسواق، ثم قرروا أن ملايين السيارات المتصلة بشبكة الإنترنت ستكون على الطريق في القريب العاجل».

وبعد مرور ثلاث سنوات، أصبح لشركة أرغوس التي يقع مقرها في تل أبيب مكاتب في ألمانيا واليابان والولايات المتحدة. وتشهد الشركة ازدهارا كبيرا في الوقت الحالي في ظل وجود قصص حول قراصنة يتحكمون في السيارات — بل وقصص عن حوادث ناتجة عن نظام القيادة الآلية في سيارات تيسلا — لفتت الانتباه إلى ضرورة تحسين أمن تكنولوجيا المعلومات في السيارات.

مرحبا بكم في إنترنت الأشياء — أشياء متصلة بشبكة تسمح لها بإرسال البيانات واستقبالها — الذي يتسع نطاقه بمرور الوقت ليشمل آلات متنوعة بدءا من أجهزة التشخيص في المستشفيات إلى ماكينات صنع القهوة والأجهزة المنزلية الأخرى. وتتوقع شركة غارتنر المحدودة، وهي شركة رائدة في مجال بحوث تكنولوجيا المعلومات وتقديم الاستشارات، ازدياد عدد الأجهزة المتصلة بالإنترنت خلال العام الحالي بنسبة ٣٠٪ ليصل إلى ٦,٤ مليار جهاز. وسيزداد كذلك حجم الإنفاق العالمي على تأمين إنترنت الأشياء بنسبة ٢٤٪ ليصل إلى ٣٤٨ مليون دولار أمريكي.

ويتيح العالم المتصل بشبكة الإنترنت فرصا جديدة لمرتكبي جرائم تكنولوجيا المعلومات لجمع بيانات شخصية تستخدم في إجراء معاملات بغرض الاحتيال أو تثبيت برامج الفدية الخبيثة — وهي برامج قادرة على تعطيل الأجهزة أو تشفير البيانات وطلب أموال مقابل إرسال مفتاح فك الشفرة.

ويقول برادلي ويسكرشن، الرئيس التنفيذي لشركة كاونت Kount، وهي شركة تعمل في مجال أمن الإنترنت يقع مقرها في مدينة بويسي بولاية أيداهو، إن هذه البرامج «نقطة اختراق جديدة للمحتالين. فهم غير مضطرين لاختراق الحاسب الآلي الخاص بي إذا كانوا يستطيعون اختراق الطابعة أو الثلاجة وجمع بيانات عني».

وغالبا ما يكون من السهل اختراق الأجهزة المنزلية المتصلة بالإنترنت لسبب بسيط، وهو أنها لا تتضمن سوى خصائص أمنية محدودة، إن لم تكن تخلو منها تماما. وشركات مثل نست لابس (Nest Labs) في بالو ألتو بكاليفورنيا، وهي تعمل في مجال صناعة أجهزة ذكية تتضمن خصائص أمنية متطورة، هي الاستثناء.

ويقول كريس كينغ، محلل مخاطر في مركز التنسيق التابع لفريق مواجهة طوارئ الحاسب الآلي، وهو جزء من معهد هندسة البرامج بجامعة كارنيغي ميلون، إن «شركات أخرى كثيرة تستخدم برامج مفتوحة المصدر وتحملها على أجهزة فحسب — دون التفكير كثيرا في النواحي الأمنية». حتى أنه يمكن اختراق الألعاب، مثل دمية هالو باربي التي يتم توصيلها بالإنترنت اللاسلكي.

وتتسع قائمة الأجهزة المعرضة للخطر مع اتساع العالم السلكي. ويقول كينغ، لقد قام قراصنة الإنترنت بتعطيل نظم التشخيص بالمستشفيات لطلب فدية. وفي غرب أوكرانيا العام الماضي، قام قراصنة الإنترنت بتعطيل شبكة كهرباء، مما تسبب في انقطاع الكهرباء عن أكثر من ٢٠٠٠٠٠ شخص. وفي ألمانيا، استهدف القراصنة مصنعا لإنتاج الصلب مما تسبب له في أضرار جسيمة.

يقوم مرتكبو جرائم تكنولوجيا المعلومات بجمع المعلومات الشخصية لإجراء معاملات بغرض الاحتيال أو تثبيت برامج طلب الفدية.

واختراق السيارات أمر مخيف للغاية نظرا لأنه قد يتسبب في حوادث مميتة. وسوف يصل عدد السيارات حول العالم التي يمكن توصيلها لاسلكيا بالإنترنت حوالي ٢٥٠ مليون سيارة بحلول عام ٢٠٢٠.

وتعمل جميع أجزاء السيارات الحديثة — الفرامل والمقود وضغط الإطارات والأضواء — من خلال أجهزة تحكم مبرمجة باستخدام الكمبيوتر ومتصلة ببعضها البعض من خلال نظام اتصال، أو «الموصل» الذي تم اختراعه منذ ٣٠ عاما قبل عصر الإنترنت. والموصل نفسه غير آمن، مثله مثل أي جزء أخر من أجزاء السيارة.

ويقول كينغ «هذا النظام لم يكن مصمما قط لتوصيله بالإنترنت، وبالرغم من ذلك تم توصيله وأصبح معرض فجأة لجميع هذه الأمور التي لم يفكر فيها مصممو السيارات من قبل».

ويتعامل مصنعو السيارات وقطع الغيار مع هذا التهديد بجدية ويتخذون تدابير أمنية معززة عقب حدوث اختراق لاثنتين من الشركات الكبرى في قطاع صناعة السيارات.

وقام الباحثون في شركة أرغوس باختراق جهاز يسمى زوبي (Zubie) يستخدم في مراقبة أداء السيارة وتوصيل بيانات فورية لاسلكيا إلى الهاتف الذكي للسائق من خلال شبكة الإنترنت، إلى جانب تنبيهات بشأن أعمال الصيانة ونصائح عن كيفية تحسين القيادة. واستطاع الباحثون لاحقا السيطرة على مقود السيارة والفرامل والمحرك. وأبلغت شركة أنغوس زوبي بأوجه القصور التي اكتشفتها والتي قالت شركة زوبي أنها قامت بمعالجتها منذ ذلك الحين.

وفي العام الماضي، سحبت شركة فيات كرايسلر للسيارات ١,٤ مليون سيارة عقب إعلان مجلة وايرد (Wired) عن قيام مجموعة من الباحثين باستخدام جهاز كمبيوتر محمول في السيطرة على سيارة جيب شيروكي من خلال الكمبيوتر الموصل بلوحة القيادة.

ويقول هيلبرون من شركة أرغوس «عندما يتم توصيل السيارات بالإنترنت، يجب حمايتها». ■

السرقة عبر الإنترنت

كان ماغنوس كارلسون في مكتبه في الطابق الثامن الذي يطل على أحد الشوارع المزدحمة في مدينة بيثيسدا بولاية ماريلاند عندما تلقى رسالة إلكترونية على جهاز الكمبيوتر الخاص به. وكان رئيسه، الرئيس التنفيذي لنقابة المهن المالية، يحتاج إلى مساعدته في تنفيذ تحويل نقدي.

ولكن عندما ضغط كارلسون على زر الرد، ظهر له عنوان غير معروف في نافذة برنامج Outlook. ويقول كارلسون «لقد عرفت منذ البداية أنها عملية احتيال تقليدية». وينبغي له أن يعرف، فجزء من وظيفته كمدير الخزانة والمدفوعات في المجموعة العالمية التي تمثل الرؤساء التنفيذيين في القطاع المالي أن يحذر الأعضاء حول العالم من مصادر الاحتيال المالي، بما في ذلك جرائم تكنولوجيا المعلومات.

وهذا النوع من أنواع الجرائم يعرف باسم «رسالة العمل المشبوهة»، ويفضل مرتكبو جرائم تكنولوجيا المعلومات استخدامها كوسيلة لدفع موظفي

السرقة عبر الإنترنت (تابع)

الشركات نحو إجراء تحويلات برقية إلى موردين أو دائنين وهميين، وعادة ما يكون ذلك من خلال محاكاة أمر قام أحد المديرين بإرساله باستخدام البريد الإلكتروني. وفي مسح لأعضاء النقابات، أشار ٦٤٪ من المجيبين إلى تلقيهم هذا النوع من رسائل العمل المشبوهة.

إصرار مرتكبي جرائم تكنولوجيا المعلومات على التسبب في أضرار قد يؤدي إلى انهيار النظام المالي العالمي بأكمله.

وهذا مجرد جانب واحد من شبكة احتيال عالمية آخذة في التوسع تتضمن عمليات وأدوات تحمل أسماء رنانة ولكنها توحي بالشرور — مثل برامج الفدية والتصيد الإلكتروني وتروجان. وقد أصبح مرتكبو جرائم تكنولوجيا المعلومات أكثر تطورا ونشاطا، فهم يعملون في وضح النهار دون خوف، ويستهدفون المؤسسات الكبيرة، مثل جي بي مورغان تشيس والخطوط الجوية البريطانية، ولجنة الانتخابات الفلبينية، ومصلحة الضرائب الأمريكية، ثم ينتقلون إلى شركات الغذاء التي تمثل فريسة أسهل عندما تخصص الشركات الكبرى مزيدا من الموارد بغرض تعزيز أمن تكنولوجيا المعلومات.

ويقول جيمس أندرو لويس، النائب الأول لرئيس مركز الدراسات الاستراتيجية والدولية في واشنطن العاصمة، والذي كتب مؤلفات كثيرة حول الاحتيال عبر الإنترنت، إن جرائم تكنولوجيا المعلومات «تتزايد بصورة مستمرة نظرا لسهولتها، وارتفاع عدد البلدان والشركات المتصلة بالإنترنت التي تطبق مناهج بدائية للحفاظ على أمن تكنولوجيا المعلومات مما يجعلها هدفا سهلا. ويوجد تفاوت كبير في إنفاذ القوانين بين مختلف بلدان العالم. ولذلك فإذا كنت قرصانا ذكيا، عليك أن تعيش في بلد لا ينفذ قوانينه».

ويقدر لويس الأضرار العالمية الناجمة عن جرائم تكنولوجيا المعلومات بأكثر من ٥٠٠ مليار دولار أمريكي سنويا — وهو ما يتجاوز إجمالي الناتج المحلي للسويد. ويتضمن هذا الرقم قيمة النقود وحقوق الملكية المسروقة، وتكلفة معالجة الاختراقات، والتأثير السلبي لجرائم تكنولوجيا المعلومات على الابتكار والتجارة والنمو الاقتصادي.

وتمثل الشركات المالية هدفا مغريا للغاية كما يتضح من سرقة ٨١ مليون دولار أمريكي من بنك بنغلاديش المركزي هذا العام. واستخدم المخترقون المعلومات الشخصية لأحد موظفي البنك في تنفيذ هذه العملية من خلال إرسال ما يزيد على ٣٦ طلب تحويل أموال إلى بنك الاحتياطي الفيدرالي في نيويورك.

وكانت الخسارة كبيرة بالنسبة لبلد في حجم بنغلاديش، ولكن شعرت الجهات التنظيمية بالقلق حيال خطر أكثر حدة، فإصرار مرتكبي جرائم تكنولوجيا المعلومات على التسبب في أضرار قد يؤدي إلى انهيار النظام المالي العالمي بأكمله، مما قد يؤدي إلى هبوط اقتصادي على غرار أزمة ٢٠٠٧–٢٠٠٨.

ويقول كريغ ميدكرافت، رئيس مجلس إدارة هيئة الأوراق المالية والاستثمارات الأسترالية إن «جرائم تكنولوجيا المعلومات تحرم المشاركين في الأسواق من استخدام أجزاء أساسية من الأسواق، وستكون على الأرجح هي الضربة القاضية التالية في العالم».

ويشير مسح للتهديدات المؤثرة على الاستقرار المالي العالمي أجرته هيئة الحفظ والمقاصة، إلى أن عددا كبيرا من المجيبين، ٢٥٪ منهم، يضعون جرائم تكنولوجيا المعلومات في مقدمة هذه التهديدات. وتمثل هذه النسبة تراجعا عن العام الماضي عندما بلغت ٤٦٪، وهو ما يعود جزئيا إلى أن المؤسسات المالية تستثمر في تدابير وقائية، ولأن مخاطر أخرى أصبحت أكثر أهمية — مثل التباطؤ في آسيا.

غير أن الجهات التنظيمية لا ترغب في المغامرة، وتلزم نظم المدفوعات وتسوية التجارة، وهي مكونات رئيسية في النظام المالي العالمي، بوضع خطط لمكافحة اختراقات أمن المعلومات ومعالجتها، وتعيين مسؤول تنفيذي للإشراف على هذه الخطط، وذلك وفقا للمبادئ التوجيهية الصادرة في يونيو عن بنك التسويات الدولية والمنظمة الدولة لهيئات الأسواق المالية.

ووفقا لمسح أجرته مؤسسة برايس ووتر كوبر، تعد جرائم تكنولوجيا المعلومات هي ثاني أكثر الجرائم شيوعا في قطاع الأعمال بعد جرائم الاختلاس. ولكن بالرغم من أن ٦١٪ من الرؤساء التنفيذيين أعربوا عن مخاوفهم إزاء جرائم تكنولوجيا المعلومات، لا تطبق خطط للمواجهة سوى في ٣٧٪ من المؤسسات.

وتنقسم جرائم الإنترنت إلى فئتين. أولا، اختراقات البيانات بغرض تحقيق كسب مادي، مثل سرقة بيانات بطاقات الهوية والدفع. أما الفئة الثانية فهي التجسس، ويندرج ضمنها سرقة أسرار المهنة واستراتيجيات التفاوض ومعلومات المنتجات.

ووفقا للتقرير الصادر سنويا عن مؤسسة سيمانتك بشأن المخاطر الأمنية على شبكة الإنترنت "Internet Security Threat Report"، ازداد عدد بطاقات الهوية المعرضة للاختراق بنسبة ٢٣٪ خلال العام الماضي ليصل إلى ٤٢٩ مليون بطاقة. ولكن قد يتجاوز الرقم الفعلي ٥٠٠ مليون بطاقة نظرا لأن شركات كثيرة لا تبلغ عن الاختراقات.

ويشير برادلي ويسكرشن، الرئيس التنفيذي لشركة كاونت، وهي شركة رائدة في تقديم حلول إدارة المخاطر الرقمية يقع مقرها في مدينة بويسي بولاية أيداهو، إلى أنه عقب حدوث اختراقات لعدد ضخم من البيانات في شركات مثل شركة أنثم (Anthem) للتأمين الصحي والسوق الرقمي eBay، أصبحت جميع بطاقات الهوية تقريبا في الولايات المتحدة الأمريكية معرضة للاختراق.

ويقول «الجميع تقريبا أصبحوا معرضين للخطر». ويتم بيع معلومات الهوية المسروقة على سوق سوداء إلكترونية مزدهرة، حيث يقوم تجار دوليون متطورون ببيع سلعهم على مواقع لمنافسة أكبر سلاسل محال التجزئة العالمية، مع إمكانية استرداد الأموال وتقديم خدمات هائلة ومعلومات عن كيفية الاستخدام.

ووفقا لمسح أجرته مؤخرا شركة آي بي إم ومعهد بونيمون على ٣٨٣ شركة في ١٢ بلدا، ارتفع متوسط تكلفة اختراق البيانات إلى ٤ ملايين دولار أمريكي من ٣,٧٩ ملايين دولار أمريكي. وكانت الاختراقات أكثر شيوعا في البرازيل وجنوب إفريقيا، وأقل شيوعا في أستراليا وألمانيا.

وفي عام ٢٠١٤، تعرض بنك جي بي مورغان تشيس في نيويورك إلى هجمة تم على إثرها اختراق بيانات ٨٣ مليون عميل، بما في ذلك الأسماء وعناوين البريد الإلكتروني والعناوين البريدية وأرقام الهواتف. وكانت هذه هي أكبر هجمة على الإطلاق تعرضت لها مؤسسة مالية في التاريخ الأمريكي، ورغم أن البنك لم يعلن عن تكلفة الاختراق، فقد أعلن عن خطط لإنفاق مبالغ إضافية على التدابير الأمنية تبلغ ٢٥٠ مليون دولار أمريكي سنويا.

ومن الصعب تقدير تكلفة سرقة حقوق الملكية الفكرية، ولكن الخسائر الاقتصادية الناجمة عن هذه السرقات قد تكون أكبر بكثير. ويقول لويس، من مركز الدراسات الاستراتيجية والدولية، إن سرقات الملكية الفكرية تأتي في صور متنوعة بدءا من تركيبة الدهانات وحتى طريقة تصنيع الصواريخ، وتؤدي إلى تقليص أرباح الابتكار. ويضيف قائلا إن «الأشخاص يبتكرون أشياء جديدة سعيا وراء تحقيق عائد مالي، وإذا لم يتحقق لهم هذا العائد، سيقومون بأمور أخرى».

والنتيجة هي تقلص حجم الاستثمارات في التكنولوجيا الجديدة وخسارة الوظائف وتراجع النمو الاقتصادي. وحتى البلدان المستفيدة تخسر في الأجل الطويل نظرا لأن الاعتماد على تكنولوجيا مسروقة يمنعها من تعلم كيفية استحداث تكنولوجيا خاصة بها. ويقول لويس «يتباطأ النمو في العالم أجمع بسبب ذلك».

ووفقا لتقديرات لويس، يبلغ متوسط التكلفة الكلية لجرائم تكنولوجيا المعلومات، بما في ذلك سرقة الملكية الفكرية، ٠,٥٪ من إجمالي الناتج المحلي العالمي. وفي البلدان مرتفعة الدخل، حيث يكون للابتكار دور اقتصادي أكبر، قد تزيد الخسائر عن ذلك لتصل إلى ٠,٩٪ من إجمالي الناتج المحلي. وتبلغ الخسائر في الاقتصادات النامية ٠,٢٪ تقريبا. ووفقا لتنبؤات شركة سايبر سيكيوريتي فينشرز، وهي شركة بحوث واستعلامات سوقية، يؤدي ذلك إلى زيادة حادة في الطلب على خدمات أمن تكنولوجيا المعلومات التي سيزداد حجمها في عام ٢٠٢٠ ليصل إلى ١٧٠ مليار دولار أمريكي مقابل ٧٥ مليار دولار أمريكي خلال العام الماضي.

وتحقق شركة كاونت زيادة سنوية في حجم معاملاتها في حدود ثلاث خانات، ويقول ويسكرشن «هذه مجرد نسبة ضئيلة من الفرص المحتملة. فأنا أعمل للأسف في قطاع متنامي للغاية.» ■

التطبيقات الرقمية وتشتت الانتباه

يتذكر لوري فوس عندما كان مبرمجا صغيرا في إحدى شركات وادي السيليكون، وأسند إليه تنفيذ مشروع روتيني غير مجد خلال شهر. ويقول «كانت مهمة غير مجدية، وقضيت وقتا طويلا على تويتر خلال هذا الشهر».

وبالنسبة لفوس الذي يشغل حاليا منصب رئيس العمليات التكنولوجية في شركته الجديدة إن بي إم، فإن استخدام تويتر أثناء العمل هو الوجه الحديث في القرن الحادي والعشرين لظاهرة قديمة قدم البحر الميت، وهي التلكؤ والمماطلة.

التشتت الناتج عن استخدام التطبيقات الرقمية والإفراط في البحث عن المعلومات يؤثران تأثيرا سلبيا متناميا على الإنتاجية.

وبالطبع تتيح التطبيقات والأدوات الحديثة سبلا جديدة لا يمكن مقاومتها تؤدي إلى ضياع الوقت. ويتعرض العاملون في مكاتبهم حول العالم إلى سيل من الأضواء والأصوات من الهواتف وأجهزة الكمبيوتر والأجهزة اللوحية. ويؤثر التشتت الناتج عن استخدام التطبيقات الرقمية والإفراط في البحث عن المعلومات تأثيرا سلبيا متناميا على الإنتاجية مع انتشار التكنولوجيا الجديدة في جميع أنحاء العالم واتساع نطاق اقتصاد المعرفة.

ووفقا لمسح صادر عن شركة كاريير بيلدر (CareerBuilder) في شهر يونيو، وهي شركة استشارات في مجال الموارد البشرية يقع مقرها في شيكاغو، يؤكد ثلاثة من كل أربعة من أصحاب الشركات ضياع ساعتين أو أكثر يوميا بسبب تشتت انتباه الموظفين.

وأشار أرباب العمل إلى استخدام الهاتف المحمول وخدمات الرسائل بوصفه العامل الأهم وراء ضياع الوقت، ويأتي بعده استخدام الإنترنت والثرثرة ووسائل التواصل الاجتماعي. ويؤدي ذلك إلى تداعيات تتضمن تدني جودة العمل وتأثر الروح المعنوية للعاملين الذين يتعين عليهم القيام بمهام زملائهم الذين لا يستطيعون التركيز في العمل بسبب استخدام التطبيقات الرقمية أو إنجاز المهام المسندة إليهم في الموعد المحدد.

ويشير ناثان زيلدس، وهو مستشار تنظيمي بالقدس، إلى أن رسائل البريد الإلكتروني من أهم أسباب ضياع الوقت، ويوجه اللوم إلى أرباب العمل لعدم قدرتهم على الحد من استخدامها. ويقول إن الموظف قد يتلقى ما بين ٥٠ و٣٠٠ رسالة مرتبطة بالعمل خلال اليوم.

ويضيف قائلا «من المستحيل قراءة جميع هذه الرسائل وفهمها. ويستمر سيل الرسائل دون توقف».

ويقول زيلدس مشيرا إلى دراسة أعدها عام ٢٠٠٦ أثناء عمله كمهندس في شركة إنتل التي تعمل في مجال صناعة رقائق الكمبيوتر، إن رسائل البريد الإلكتروني وغيرها من وسائل تشتيت الانتباه تكلف العامل العادي يوما كاملا بدون إنتاجية كل أسبوع. ويؤدي ذلك إلى خسائر بقيمة مليار دولار أمريكي سنويا بالنسبة لشركة يعمل بها ٥٠٠٠٠ عامل.

ومن الصعب مقاومة قراءة رسائل البريد الإلكتروني. فالموظف يشعر بأنه مضطر لقراءة الرسائل والرد عليها في أي وقت خلال النهار أو الليل خوفا من عدم الرد على رسالة مهمة أو رغبة في إثارة إعجاب زملائه أو رئيسه.

ويقول «هذا أشبه بأزمة السجين. فالجميع يرغبون في إرسال رسائل أقل والعودة إلى منازلهم مبكرا. ولكن لا يجرؤ أي منهم على أن يكون أول من يبادر بذلك».

وتستخدم غلوريا مارك، أستاذة علم النفس التي تدرس بقسم علوم المعلومات بجامعة كاليفورنيا بمدينة إرفاين، تشبيه المقامرة لتؤكد أن الجميع مهيؤون لاستخدام الرسائل الإلكترونية.

وتقول «أصف ذلك باسم ظاهرة لاس فيغاس». فاللاعب على ماكينة المقامرة يحصل على مكافآت نقدية متفرقة على فترات عشوائية. وتوقع الحصول على مكافأة أخرى كفيل بأن يجعل اللاعب يستمر في اللعب.

وتضيف قائلة «إن السلوكيات المفروضة عشوائيا هي الأصعب في معالجتها».

وفي دراسة أعدتها غلوريا مارك عام ٢٠١٢، توصلت إلى أن العاملين يمكنهم التركيز على شاشة الكمبيوتر لمدة ٧٥,٥ ثانية في المتوسط فقط قبل أن يتشتت انتباههم بفعل أمور أخرى. وفي العام الماضي، تراجع هذا الرقم إلى ٤٧ ثانية.

وقد استخدم العاملون ورؤساؤهم استراتيجيات متنوعة لمكافحة تشتت الانتباه وفرط البحث عن المعلومات. ويخصص الكثيرون أوقاتا محددة لقراءة الرسائل ويتجاهلون صندوق الرسائل الواردة لبقية اليوم.

ويقول فوس من شركة إن بي إم «أقضي وقتا طويلا في تنظيم بريدي الإلكتروني». والحل من وجهة نظره هو «الإصرار على تجاهل» أي رسائل «مكررة أو روتينية أو أي رسائل لا أحتاج إلى معرفة فحواها أو التعامل معها».

ويقول كليف ويليامز، مصمم كبير في شركة نكست دور (Nextdoor)التي يقع مقرها في سان فرانسيسكو والتي تصف نفسها بأنها «الشبكة الاجتماعية الخاصة الأقرب إليك»، «ينبغي إغلاق جميع الإشعارات. لا تدعها تظهر أمامك فجأة لتشتت انتباهك».

غير أن ويليامز يعترف بأن تجنب عوامل تشتيت الانتباه هو «صراع مستمر».

ويقول «إن الأمر مشابه لخسارة الوزن. فأنت تخسر بعضا من وزنك لتكتسب بعض الوزن لاحقا». ■

كريس ويليش صحفي مالي في واشنطن العاصمة.