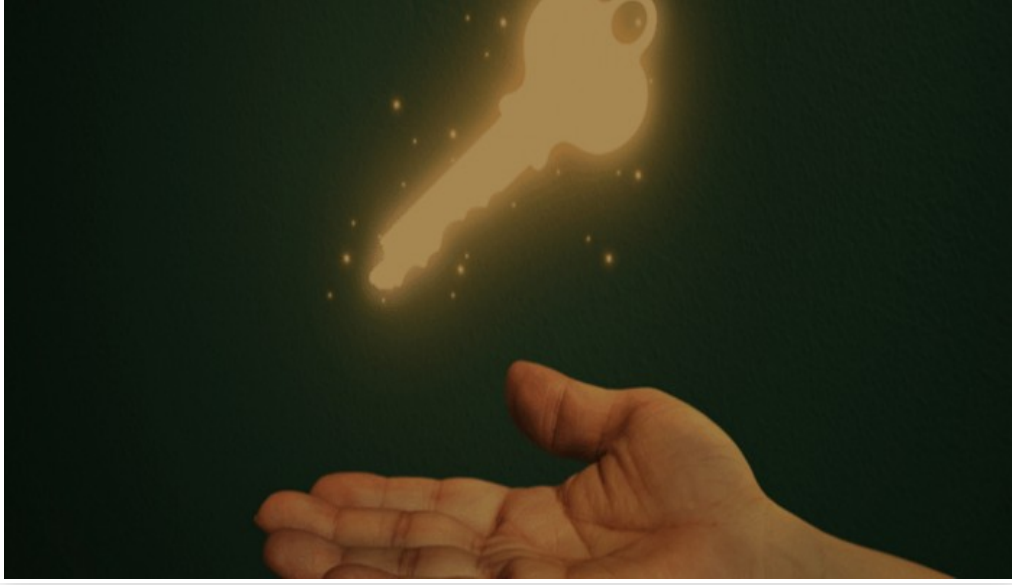


كلمات المرور الضعيفة قد تنتهي بسرقة حسابات اللاعبين عبر الإنترنت



الخميس 1 فبراير 2018 08:02 م

سرعان ما أصبحت الألعاب التي تُمارس عبر الإنترنت صناعة مربحة للغاية، مع امتلاك عدد أكبر من المستخدمين حسابات ألعاب عبر الإنترنت [] ووفقاً لدراسة استطلاعية أجرتها كاسبرسكي لاب، فإن 71 في المئة من الأشخاص الذين شملهم الاستطلاع في دولة الإمارات يمارسون بانتظام ألعاباً عبر الإنترنت، وهي نسبة ترتفع إلى 76 في المئة لدى الفئة العمرية التي تتراوح بين 25 و34 عاماً، وإلى 74 في المئة لدى من تتراوح أعمارهم بين 16 و24 عاماً [] ومن المرجح أن تعود حسابات الألعاب الإلكترونية عبر الإنترنت بالربح على مجرمي الإنترنت، إذ يمكنهم بيع الحسابات المخترقة في السوق السوداء [] وعلى الرغم من التهديدات الإلكترونية المحدقة باللاعبين، فإنهم غالباً ما يتركون حساباتهم عُرضة لمحاولات القرصنة، ما يُعرض إنجازاتهم في اللعب وبيانات الشخصية وربما دخلهم المادي للخطر []

ويقدّر حجم الجمهور العالمي المتنامي في عالم الألعاب الإلكترونية، والذي يتصدره اللاعبون على منصات الإنترنت، مثل "ستيم" Steam وبلاي ستيشن نتورك PlayStation Network وإكس بوكس لايف Xbox Live، بين 2.2 مليار و2.6 مليار لاعب [] وهذا يجعل قطاع الألعاب الإلكترونية عبر الإنترنت هدفاً محددًا لمجرمي الإنترنت الذين يأملون في تعطيل العمليات على الإنترنت وسرقة بيانات مثل كلمات المرور ومعلومات البطاقات المصرفية، وهو ما يظهر بوضوح من الهجمات الأخيرة على منصات إكس بوكس وبلاي ستيشن []

ويسعى مجرمو الإنترنت إلى الوصول إلى مجموعة هائلة من الأهداف المحتملة للاختيار من بينها، في ظلّ الأرقام التي تشير إلى ممارسة أكثر من نصف مستخدمي الإنترنت الألعاب بانتظام على الإنترنت [] وعلاوة على ذلك، أصبحت الألعاب تشكل جانباً مهماً من حياة كثير من المستخدمين الذين يتوجهون إلى الألعاب عندما يشعرون بالملل أو الوحدة وللتسلية مع أصدقائهم عبر الإنترنت، وبالتالي، يمكن أن تتسبب الهجمات الناجحة بإزعاج بالغ لضحاياها الذين قد يتأثرون نفسياً بفقد إمكانية الوصول إلى حسابات ألعابهم المفضلة مؤقتاً أو نهائياً فضلاً عن سرقة بياناتهم، وذلك جرّاء خسارة ساعات أو أيام عديدة من الإنجاز المحقق والتقدم المحرز في الألعاب وفي بناء ملفاتهم الشخصية، علاوة على أية أموال قد يكونون وضعوها في تلك الحسابات []

وقال 18 في المئة ممن شملتهم الدراسة الاستطلاعية في دولة الإمارات، وممن تعرض أحد حساباتهم الخاصة بالألعاب على الإنترنت لمحاولات هجوم أو هجمات ناجحة، إن حساباتهم "هدف لمجرمي الإنترنت"، وهي نسبة ترتفع إلى 23 في المئة لدى الرجال []

وبدلاً من كون الألعاب نشاطاً يقتصر على المنزل، أصبحت تُمارس في مختلف أوقات الحياة اليومية لدى العديد من المستخدمين، وهو ما يتضح من حقيقة أن ما يقرب من 40 في المئة من المستطلعة آراؤهم في دولة الإمارات يستخدمون الهواتف الذكية لممارسة الألعاب على الإنترنت، الأمر الذي يبيّن الأهمية البالغة التي تحظى بها حسابات الألعاب عند أصحابها [] ويستخدم ما يقرب من 30 في المئة من المستخدمين شبكات الإنترنت اللاسلكية العامة لتسجيل الدخول إلى حسابات الألعاب الخاصة بهم، في حين يقول 51 في المئة إنهم لا يتخذون أية تدابير أمنية إضافية عند استخدام هذه الشبكات، وذلك على الرغم من أن الهواتف الذكية ليست آمنة بطبيعتها، الأمر الذي يعرضهم لمخاطر أمنية واضحة [] ومما يزيد من الخطر أن 10 في المئة فقط من المستخدمين اعتبروا حساب الألعاب أحد ثلاثة حسابات تتطلب وضع كلمات مرور قوية لحمايتها []

وعلاوة على ذلك، قد يفقد الضحايا بسهولة قُدرتهم على الوصول إلى العديد من حساباتهم الأخرى، مثل البريد الإلكتروني وحسابات وسائل التواصل الاجتماعي، نظراً للترابط القائم اليوم بين العديد من الملفات الشخصية على الإنترنت [] وفيما قد يتسبب هذا أحياناً بأضرار نفسية للمستخدمين الذين يمارسون الألعاب بغرض الترفيه، يمكن أن يُحدث أضراراً جسيمة للاعبين المحترفين الذين يجني بعضهم المال من اللعب []

وقال أندري موكولا، رئيس قسم الأعمال التجارية للمستهلكين لدى كاسبرسكي لاب: "إن وجود كنز من المعلومات الشخصية المتاحة على الإنترنت يتيح لمجرمي الإنترنت فرصاً سانحة أكثر من أي وقت مضى للاستيلاء على البيانات الخاصة بالمستخدمين، والتي يمكن بيعها في السوق السوداء الرقمية، موضحاً أن اللاعبين الهواة والمحترفين على الإنترنت يشعرون بالقلق حيال إمكانية اختراق حساباتهم أو حتى

عدم التمكّن من الوصول إليها جرّاء نسيان كلمات المرور.”

وأضاف موكولا: “هذه هي المعضلة التي تواجه المستخدمين كل يوم، جرّاء إقدام كثير منهم على أقل الخيارات أمناً والمتمثل باستخدام كلمة المرور نفسها لجميع الحسابات، أو كلمات مرور بسيطة يسهل على القرصنة تخمينها] ومع ذلك، لن يكون المستخدمون مطمئنين إلى سلامة حساباتهم وتمتعها بالحماية وعدم ضياع جهودهم وإنجازاتهم أدرج الرياح، إلا إذا اتخذوا الاحتياطات المناسبة واستخدموا كلمات مرور قوية ومختلفة لكل حساب”.

تجدر الإشارة إلى أن العديد من منتجات كاسبرسكي لآب تتضمن أدوات لإدارة كلمات المرور من أجل مساعدة المستخدمين في الحفاظ على أمن بياناتهم، مثل أداة Kaspersky Password Manager المتاحة في الحل Kaspersky Total Security. وتقوم هذه الأداة بتخزين جميع كلمات المرور في قبو رقمي آمن، متيحة سهولة الوصول إليها من أجهزة الحاسوب وأجهزة ماك ومن الهواتف الذكية] وتقوم أداة خاصة بإنجاز الجزء الشاق من العمل عبر التأليف التلقائي لكلمات مرور قوية ومرنة، بينما لا يحتاج المستخدم إلّا إلى تذكّر كلمة مرور رئيسية واحدة من أجل الوصول إلى جميع حساباته على الإنترنت] ويمكن للمستخدم التحقق من مدى قوة كلمات المرور التي يستخدمها حالياً عبر زيارة الموقع Password Check التابع لكاسبرسكي لآب]