دراسة: كلمات المرور المعتمدة على الصورة ليست أقل أمناً

قد لا يكون أمن كلمات المرور المعتمدة على الصورة ضعيفاً كما اعتقد الكثيرون في البداية، حيث يمكن لهذا النوع من أنواع كلمات المرور أن يكون صعباً على الاختراق بحسب طريقة استخدامه، وذلك بحسب ما ذكرت دراسة حديثة.

وبدأ الحديث عن كلمات المرور المعتمدة على الصورة منذ اعتمادها في نظام التشغيل ويندوز 8 كأحد خيارات الحماية، حيث يستطيع المستخدم اختيار صورة ما ثم الولوج إلى النظام عبر النقر على نقاط معينة ضمن الصورة أو رسم الدوائر والخطوط حول مناطق معينة ضمن الصورة يحددها المستخدم.

وذكرت الدراسة التي نشرها "باول دوكلين" الباحث في شركة "سوفوس" المتخصصة بحلول الأمن الرقمي، بأن كلمات المرور المعتمدة على الصورة ليست أقل أمناً من أنواع كلمات المرور الأخرى، حيث يمكن لكلمة المرور المعتمدة على الصورة أن تكون قوية للغاية.

وقال "دوكلين" في دراسته بأن كلمات المرور المعتمدة على الصورة يمكن لها أن تكون ضعيفة، لكن هذا يعتمد على عدد "الإيماءات" التي يتم استخدامها وعدد "نقاط الاهتمام" الموجودة في الصورة. ويصير مصطلح "نقطة الاهتمام" إلى وجوه الأشخاص أو الحيوانات أو الأبنية وغير ذلك من العناصر الموجودة في الصورة والتي يقوم المستخدمون عادةً باختيارها كنقاط للنقر عليها أو رسم الدوائر حولها لفتح

الجهاز.

وأوضحت الدراسة بأن مايكروسوفت قد طورت معادلة للتوصل إلى عدد كلمات المرور الممكن استخراجها من صورة واحدة اعتمادًا على الإيماءات بها ونقاط الاهتمام. وبالتالي فكلما كانت نقاط الاهتمام والإيماءات أكثر في الصورة، كلما ازداد أمر كلمة المرور بشكل كبير.

وأشارت الدراسة بأن نوع الإيماءات المستخدمة فوق الصورة يمكن أن تزيد صعوبة تقليدها. فالدائرة على سبيل المثال أصعب من النقرة، والخط أكثر صعوبة من الدائرة. وبالتالي فإن كلمة مرور تتألف من خمس إيماءات، جميعها من النقرات، ستكون أسهل للتخمين من كلمة مرور تتألف من خمس إيماءات كلها من الخطوط.

يُذكر أن استخدام كلمة المرور المعتمدة على الصورة في ويندوز 8 لا تلغي أيضًا وجوب تحديد كلمة مرور تقليدية يتم اللجوء إليها في حال فشل المستخدم في الولوج إلى النظام بعد خمس محاولات فاشلة.