

جوجل تتخلي عن الشيفرات المرسله بـ SMS وتستبدلها بنظام 2SV الجديد ☐ هذه مميزاتة



الجمعة 4 أغسطس 2017 03:08 م

خلال هذا الشهر، بدأت جوجل بإثاء المستخدمين عن استقبال شيفرات تطبيق التحقق بخطوتين 2SV عن طريق خدمة الرسائل القصيرة SMS.

وبدأ ذلك خلال الأسبوع الماضي، فعندما تحاول الدخول إلى حسابك الشخصي، قد تتلقى دعوةً من جوجل للبدء في استقبال الرسائل عن طريق تطبيق جوجل بدلاً من الشيفرات التي تتكون من 6 أرقام عن طريق تطبيق الرسائل النصية، بحسب موقع Cnet المتخصص في أخبار التكنولوجيا ☐

وتقوم جوجل بهذا التحرك؛ نظراً إلى أن الرسائل الجديدة أكثر تأمناً من خدمة الرسائل النصية SMS. كما تعمل هذه الرسائل على تسهيل وتسريع عملية الدخول إلى الحساب الشخصي ☐ وبمناسبة إطلاق هذه الخدمة الجديدة، راود أذهان المستخدمين بعض الأسئلة بشأنها، والتي أجاب عنها تقرير Cnet.

ما هو التحقق بخطوتين 2SV؟

يُضيف تطبيق التحقق بخطوتين Two-Step Verification (الذي يُشار إليه بـ 2SV إذا أردت اختصاره، رُغم أنه يُطلق عليه أيضاً عامل التوثيق الثنائي Two-Factor Authentication أو 2FA) طبقة من التأمين للحسابات الشخصية على الإنترنت، بدءاً من أمازون وآبل وجوجل، وصولاً إلى فيسبوك وإنستغرام وتويتر ☐ وبدلاً من استخدام كلمة المرور فقط للدخول إلى الحساب، تحتاج أيضاً إلى إدخال كلمة المرور الخاصة بك وهو عامل التحقق الأول، ثم بعد ذلك إدخال رمز يجري إرساله عن طريق خدمة الرسائل القصيرة SMS أو رسالة عن طريق تطبيق التوثيق وهو العامل الثاني ☐ وهذا يعني أن المخترق بحاجة إلى سرقة كل من كلمة المرور والهاتف؛ كي يتمكن من الولوج إلى حسابك الشخصي ☐

إذاً، لماذا الابتعاد عن خدمة الرسائل القصيرة SMS؟

يعتبر استقبال شيفرات أو رموز التحقق بخطوتين 2SV عن طريق خدمة الرسائل القصيرة SMS أقل أماناً من استخدام تطبيق التوثيق ☐ وتمكّن المخترقون من خداع الحامل؛ كي ينقل رقم الهاتف إلى جهاز جديد، في خطوة يُطلق عليها تبادل بطاقة تعريف المشترك SIM. ويمكن لهذا الأمر أن يكون بسهولة التعرف نفسها على رقم الهاتف الخاص بك والأرقام الأربعة الأخيرة من رقم التأمين الاجتماعي، وذلك من خلال البيانات التي يجري تسريبها من وقت لآخر من البنوك والمؤسسات الكبيرة ☐ وإذا ما تمكن المخترق من إعادة توجيه رقم الهاتف، فلن يكون بحاجة إلى هاتفك كي يتمكن من الدخول إلى شيفرات أو رموز التحقق بخطوتين 2SV.

وبالإضافة إلى هذا، إذا قمت بمزامنة الرسائل النصية مع الحاسوب المحمول أو الجهاز اللوحي، يُمكن للمخترق أن يدخل إلى رموز خدمة الرسائل القصيرة SMS عن طريق التماسي مع الجهاز الذي يمتلكه ☐

وبعد ذلك، يتعرض الجهاز لخلل في نظام الاتصال الخاص بالهاتف ☐ وعن طريق ما يُطلق عليه هجوم نظام الإشارة SS7، يُمكن للمخترق أن يتجسس عن طريق نظام الهاتف الجوال، والاستماع إلى الاتصالات واعتراض الرسائل النصية والتعرف على موقع هاتفك ☐

وتعتبر جميع السيناريوهات السابقة ضمن الأخبار السيئة لهؤلاء الذين يستقبلون شيفرات أو رموز التحقق بخطوتين 2SV عن طريق خدمة الرسائل القصيرة SMS.

ما البديل الذي ينبغي علي استخدامه؟

يمكن استخدام تطبيقات التوثيق، مثل Google Authenticator أو Microsoft Authenticator أو Authy. وتتمتع هذه التطبيقات بعدم احتياجها إلى الاعتماد على حائك؛ فالشيفرات تظل مع التطبيق حتى لو تمكن المخترق من نقل رقمك إلى هاتف جديدٍ وتنتهي صلاحية الشيفرات أو الرموز سريعاً، عادةً بعد مرور 30 ثانية أو شيء من هذا القبيل.

وبالإضافة إلى كونك تتمتع بنظام حماية أقوى من خدمة الرسائل القصيرة SMS، يعتبر تطبيق التوثيق أسرع؛ وتحتاج فقط إلى الضغط على زر لتأكيد هويتك بدلاً من المتاعب التي تواجهها عند إدخال الرمز المكون من 6 أرقام يدوياً.

ما هي رسائل جوجل؟

يسمح لك خيار رسائل جوجل Google Prompt بتلقي الشيفرات أو الرموز دون استخدام خدمة الرسائل القصيرة SMS أو تطبيق توثيق منفصل. ويدخل هذا التطبيق ضمن تطبيق Google Now على نظام أندرويد وكذلك ضمن تطبيق Google Search على نظام iOS. تعلم كيفية تثبيت Google Prompt.

هل أنا بحاجة إلى 2SV إذا كانت خدمة الرسائل القصيرة ضعيفة للغاية؟

نعم، فبالإضافة إلى وضع كلمات مرور قوية واستخدام كلمات مرور مختلفة لكل حساب من حساباتك، يعتبر تثبيت تطبيق التحقق بخطوتين 2SV الخطوة الأفضل التي يمكنك اتخاذها لتأمين حساباتك على الإنترنت، حتى ولو أصرت على استقبال الشيفرات والرموز عن طريق خدمة الرسائل القصيرة SMS.

كما يعتبر التحقق بخطوتين عن طريق خدمة الرسائل القصيرة SMS أفضل من التحقق من خلال خطوة واحدة؛ إذ يحتاج المخترق إلى الحصول على أو تخمين كلمة المرور فقط؛ كي يتمكن من الدخول إلى بياناتك. فلا تجعل حسابك مثل الثمار المتدلية المعرضة للاستهداف بسهولة من قبل المخترقين.

لكن، يعتبر التحقق بخطوتين 2SV أمراً مثيراً للمتاعب

يعد التطبيق أقل إثارةً للمتاعب عند استخدامه بالشكل الصحيح واستقبال الرموز والشيفرات عن طريق رسائل جوجل Google Prompt أو تطبيق للتوثيق لا تحتاج فيه إلى إدخال رمز يتكون من 6 أرقام. وبالتأكيد، يجبرك بعدها على اتخاذ خطوة أخرى تتعلق بالسحب والضغط على الهاتف بعد إدخال كلمة المرور للدخول إلى أحد حساباتك.

ومع ذلك، يمكن القول إن متاعب الخطوة الثانية في تطبيق التحقق بخطوتين 2SV تتلاشى أمام المتاعب التي نواجهها عندما يجري اختراقنا. وفي أحسن الأحوال، يعتبر تعرُّضنا للاختراق ضمن المتاعب، وغالباً ما يعتبر هذا مزيجاً من الغضب والألم والارتباك. وعموماً إذا تعرضت للاختراق، يمكنك استرداد حسابك استرداد حساب Google المخترق أو المسروق من خلال هذه الخطوات، والمنشورة على موقع جوجل.