

واتساب يعزز حماية الحسابات بكلمات مرور معقدة وبيانات عن المتصل



الخميس 27 أغسطس 2026 08:30 م

يشهد تطبيق واتساب تحديثات متتالية تستهدف تعزيز مستوى الأمان وحماية حسابات المستخدمين من محاولات الاختراق والوصول غير المصرح به، وفي أحدث خطواته بهذا الاتجاه، أتاحت شركة ميتا إمكانية استخدام كلمات مرور أكثر تعقيدًا ضمن ميزة التحقق بخطوتين، بدلاً من الاعتماد فقط على رمز التعريف الشخصي التقليدي المكون من ستة أرقام

ويعمّن التحديث مستخدمي واتساب خيارًا إضافيًا لتأمين حساباتهم، من خلال إنشاء كلمة مرور تجمع بين الحروف والأرقام، مع إمكانية الاستعانة بالرموز الخاصة، بما يجعل عملية تخمين بيانات الدخول أكثر صعوبة، خاصة بالنسبة إلى المستخدمين الذين اعتادوا اختيار أرقام قصيرة أو متوقعة لحماية حساباتهم

كلمات مرور أكثر تعقيدًا لحماية الحساب

وبموجب التحديث الجديد، لم يعد المستخدم مضطّرًا إلى الاكتفاء برمّز مكون من ستة أرقام عند تفعيل التحقق بخطوتين، إذ أصبح بإمكانه اختيار كلمة مرور أكثر قوة، على أن تتكون من 8 خانات على الأقل، وتضم حرفًا واحدًا على الأقل ورقمًا واحدًا على الأقل

كما يتيح النظام استخدام الرموز الخاصة، وهو ما يمنح المستخدم مساحة أكبر لإنشاء كلمة مرور يصعب تخمينها مقارنة بكلمات المرور البسيطة أو الرموز الرقمية المتكررة

وتأتي هذه الخطوة في وقت أصبحت فيه حماية الحسابات الرقمية أكثر أهمية، خصوصًا مع تزايد محاولات الاختتيال الإلكتروني وسرقة الحسابات واستغلال كلمات المرور الضعيفة للوصول إلى بيانات المستخدمين أو انتحال هويتهم أمام جهات الاتصال الخاصة بهم

ولا يعني طرح كلمات المرور الجديدة إلغاء خيار التحقق بخطوتين، بل يمثل تطويرًا لطريقة تأمين الحساب ومنح المستخدمين وسيلة أكثر مرونة لإنشاء بيانات حماية قوية

لماذا تعد كلمة المرور الأقوى مهمة؟

يعتمد مستوى حماية أي حساب رقمي بدرجة كبيرة على مدى صعوبة تخمين بيانات الدخول الخاصة به، ولذلك فإن استخدام تسلسلات رقمية سهلة أو معلومات شخصية معروفة قد يجعل الحساب أكثر عرضة لمحاولات التخمين

أما الجمع بين الحروف والأرقام والرموز، فيزيد من عدد الاحتمالات الممكنة لكلمة المرور، وهو ما يجعل اكتشافها أكثر صعوبة عند مقارنتها برمّز رقمي قصير

ومن هنا، يمثل التحديث الجديد محاولة لتشجيع مستخدمي واتساب على الاعتماد على بيانات حماية أكثر تعقيدًا، خصوصًا أولئك الذين يستخدمون الحساب في التواصل الشخصي أو العمل ويحتفظون من خلاله بمحادثات وملفات وصور ومعلومات قد تكون مهمة أو حساسة

وتظل الميزة اختيارية، ما يعني أن المستخدم يستطيع اختيار الطريقة التي تناسبه في تأمين حسابه، إلا أن استخدام كلمة مرور قوية يظل من الإجراءات المهمة لتقليل مخاطر الوصول غير المصرح به

واتساب يوسع خيارات الحماية على الأجهزة المتعددة

ولم تقتصر التغييرات على طريقة إنشاء كلمة المرور، إذ شهدت إدارة الحسابات على الأجهزة المتعددة أيضًا مزيدًا من المرونة

ويستطيع المستخدمون الذين يعتمدون على الحساب نفسه عبر أكثر من جهاز إدارة كلمات المرور الخاصة بالحساب من داخل إعدادات واتساب، سواء على أجهزة أندرويد أو آيفون، وذلك من خلال الدخول إلى قسم الحساب ثم الوصول إلى إعدادات كلمات المرور

ويعكس ذلك توجه التطبيق إلى توفير أدوات أمنية أكثر تكاملًا بدلًا من حصر حماية الحساب في خطوة واحدة، خاصة مع استخدام واتساب على الهواتف وأجهزة أخرى في الوقت نفسه

ويأتي دعم الأجهزة المتعددة في ظل تغير طريقة استخدام تطبيقات المراسلة، إذ لم يعد المستخدم يعتمد بالضرورة على هاتف واحد فقط، وإنما قد ينتقل بين أكثر من جهاز خلال اليوم، الأمر الذي يجعل إدارة وسائل الحماية بصورة واضحة ومباشرة أمرًا أكثر أهمية

معلومات جديدة عند تلقي مكالمات من أرقام مجهولة

وفي تحديث أمني آخر، بدأ واتساب في تقديم معلومات إضافية للمستخدم عند تلقي مكالمات من أرقام غير محفوظة في قائمة جهات الاتصال

وتتيح الميزة للمستخدم الاطلاع على معلومات سياقية مرتبطة بالمتصل، من بينها الدولة التي ينتمي إليها الرقم، إلى جانب معرفة ما إذا كان هناك أعضاء في مجموعات دردشة مشتركة بين المستخدم والمتصل

وقد تساعد هذه المعلومات في إعطاء المستخدم صورة أوضح عن هوية المتصل قبل اتخاذ قرار بالرد على المكالمة أو تجاهلها، خاصة عندما يكون الرقم غير معروف ولا يظهر ضمن جهات الاتصال

وتكتسب هذه الخاصية أهمية خاصة مع انتشار المكالمات غير المرغوب فيها ومحاولات الاحتيال التي قد تعتمد على أرقام مجهولة لجذب انتباه المستخدم أو دفعه إلى مشاركة معلومات شخصية أو مالية

كيف يمكن أن تساعد المعلومات الإضافية في مواجهة الاحتيال؟

في كثير من الحالات، يمثل الاتصال من رقم غير معروف نقطة البداية لمحاولة احتيال أو خداع، خصوصًا عندما يحاول المتصل إقناع المستخدم بأنه شخص يعرفه أو جهة يتعامل معها

ومن خلال إظهار الدولة المرتبطة بالرقم والمجموعات المشتركة، يمنح واتساب المستخدم بعض المؤشرات التي يمكن أن تساعد في تقييم المكالمة قبل التفاعل معها

فعلى سبيل المثال، وجود رقم من دولة غير متوقعة بالنسبة إلى المستخدم قد يمثل مؤشرًا يستحق الانتباه، بينما يمكن لوجود مجموعات مشتركة أن يوفر سياقًا إضافيًا حول كيفية وصول المتصل إلى المستخدم

ومع ذلك، فإن ظهور هذه المعلومات لا يعني بالضرورة أن المكالمة آمنة أو أن المتصل موثوق، إذ تظل مسؤولية التحقق من هوية الشخص أو الجهة المتصلة أمرًا مهمًا، ولا ينبغي مشاركة كلمات المرور أو رموز التحقق أو البيانات المصرفية مع أي متصل مجهول

الميزة الجديدة متاحة حاليًا على أندرويد

وبحسب المعلومات المتاحة عن التحديث، فإن خاصية عرض المعلومات الإضافية عند تلقي مكالمات من أرقام غير محفوظة تتوفر حاليًا على أجهزة أندرويد، في إطار طرح تدريجي لمزايا الأمان الجديدة داخل التطبيق

وقد تختلف إتاحة بعض الميزات من مستخدم إلى آخر وفقًا لإصدار التطبيق ونظام التشغيل ومرحلة طرح التحديث، لذلك قد لا تظهر جميع الخيارات الجديدة لدى المستخدمين في الوقت نفسه

ويعني ذلك أن عدم ظهور الميزة مباشرة لا يشير بالضرورة إلى وجود مشكلة في الحساب، إذ قد تحتاج بعض الخصائص إلى تحديث التطبيق أو الانتظار حتى يصل التحديث إلى الجهاز

حماية الحساب لم تعد تعتمد على خطوة واحدة

ويكشف التحديث الأخير عن اتجاه متزايد لدى واتساب نحو التعامل مع أمن الحساب باعتباره منظومة متكاملة، بدلاً من الاعتماد على إجراء واحد فقط

فإلى جانب التحقق بخطوتين، يعمل التطبيق على إضافة أدوات تساعد المستخدم على التعامل مع المكالمات غير المعروفة، وفهم سياق الاتصال، وإدارة وسائل حماية الحساب من الأجهزة المختلفة

وتزداد أهمية هذه الإجراءات مع ارتفاع الاعتماد على تطبيقات المراسلة في التواصل اليومي، إذ أصبحت الحسابات تحمل كميات كبيرة من البيانات الشخصية، بداية من المحادثات والصور، وصولاً إلى المستندات وبيانات العمل والمعلومات المرتبطة بالعائلة والأصدقاء

وفي حال تمكن شخص غير مصرح له من الوصول إلى الحساب، فقد لا تقتصر المخاطر على قراءة الرسائل، بل قد تمتد إلى محاولة التواصل مع جهات الاتصال باسم صاحب الحساب، أو استغلال المحادثات والبيانات الموجودة داخله

نصائح للاستفادة من التحديث الجديد

ولتحقيق أكبر استفادة من أدوات الحماية الجديدة، يمكن للمستخدم اتباع مجموعة من الإجراءات الأساسية، في مقدمتها اختيار كلمة مرور طويلة ومعقدة، وعدم استخدام تاريخ الميلاد أو رقم الهاتف أو الأرقام المتكررة ضمن كلمة المرور

كما يُنصح بعدم استخدام كلمة المرور نفسها في أكثر من خدمة، حتى لا يؤدي اختراق حساب آخر إلى تعريض حساب واتساب للخطر

ويجب أيضاً عدم مشاركة كلمة المرور أو رموز التحقق مع أي شخص، حتى لو ادعى أنه من فريق الدعم أو جهة رسمية، إلى جانب تجنب الضغط على الروابط المشبوهة التي تصل عبر الرسائل أو المكالمات

وفي حالة تلقي مكالمة من رقم غير معروف، يمكن للمستخدم الاستفادة من المعلومات التي يعرضها واتساب، لكن مع التعامل معها باعتباره مؤشرات مساعدة وليست ضماناً كاملاً لهوية المتصل