

أمن المعلومات والمواقع الإلكترونية

الإجراءات والخطوات



Firewall Summary: Attacks Blocked for uobaghdad.edu.iq/

Block Type	Complex	Brute Force	Blocklist	Total
Today	199	17	557	773
Week	3,035	177	14,294	17,506
Month	13,419	1,813	114,804	130,036

- **Complex**: هو عندما يقوم الزائر بتقديم طلب إلى موقعك مصمم خصيصًا لاستغلال موقعك أو العثور على ثغرة يمكنه استغلالها لاحقًا. تحظر Firewall هذه الأنواع من الهجمات.
- **Brute Force Attack**: هي محاولات تخمين لتسجيل الدخول باسم المستخدم / كلمة المرور. تهدف هذه الهجمات إلى تسجيل الدخول إلى مسؤول WordPress الخاص بموقعك. يحظر موقعك أي IP إذا قام بعشر محاولات خاطئة لحزر اسم المستخدم او كلمة المرور لمدة 6 ساعات.
- **Blocklists Blocks**: هي عدد المرات التي تم فيها منع IP بشكل استباقي من الوصول إلى موقعك تمامًا

الإجراءات المتبعة

- استخدام بروتوكول HTTPS، أي "بروتوكول نقل الروابط النصية بأمان". يعمل بروتوكول HTTPS على ترميز الاتصال بين متصفح المستخدم وموقعك الإلكتروني، بما يساعد في حماية المعلومات المرسلة والمستلمة من خلال تعصيب إمكانية التنصت عليها واعتراضها حتى إن لم تكن تتعامل مع معلومات حساسة. وذلك لأن أي معلومات حول زيارة ما إلى الموقع الإلكتروني قد تكشف تفاصيل حساسة عن الزائر. على سبيل المثال، إذا كان موقعك الإلكتروني يتضمن حقولاً نصية مفتوحة، قد يدخل المستخدم، عن طريق الخطأ، تفاصيل الاتصال به أو أي بيانات أخرى قد تهدد أمانه إذا وصلت إلى الأيدي الخطأ. وإلى جانب أمان موقعك الإلكتروني. يمكن لاستخدام بروتوكول HTTPS أن يرفع ترتيب موقعك الإلكتروني على محركات البحث (مؤشر إيجابي)
- استخدام SSL والذي يقوم بتشفير البيانات. يؤدي كل من HTTPS و SSL نفس الشيء المتمثل في جعل المعاملات والمحادثات عبر الإنترنت أكثر أماناً وتشفيراً.



الإجراءات المتبعة

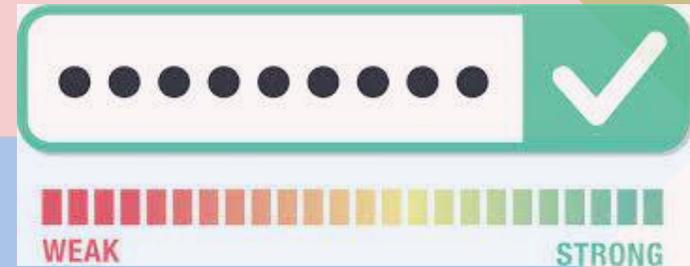
- Wordfence وهو جدار حماية (Firewall) لنقطة النهاية (endpoint) وماسح ضوئي للبرامج الضارة لحماية WordPress تعمل ميزة Threat Defense Feed على تزويد Wordfence بأحدث قواعد جدار الحماية وتوقيعات البرامج الضارة (malware signatures) وعناوين IP الضارة التي يحتاجها للحفاظ على الموقع. يعد Wordfence، الذي يقدم مجموعة من الميزات الإضافية مثل: (CAPTCHA, 2FA) أكثر طول أمان WordPress المتاحة.
- Cloudflare عبارة عن شبكة عالمية مصممة لجعل كل اتصال بالإنترنت آمناً وخاصاً وسريعاً وموثوقاً، يعمل أيضاً على تسريع تحميل الصفحة وتحسين مُحسّنات محرّكات البحث SEO والحماية من هجمات DDoS ونقاط الضعف الخاصة بـ WordPress وهو أيضاً شبكة توصيل المحتوى (content delivery network) والتي هي عبارة عن شبكة موزعة من الخوادم توفر العديد من المزايا لموقع الويب مثل التخزين المؤقت لمحتوى موقع الويب



CLOUDFLARE®

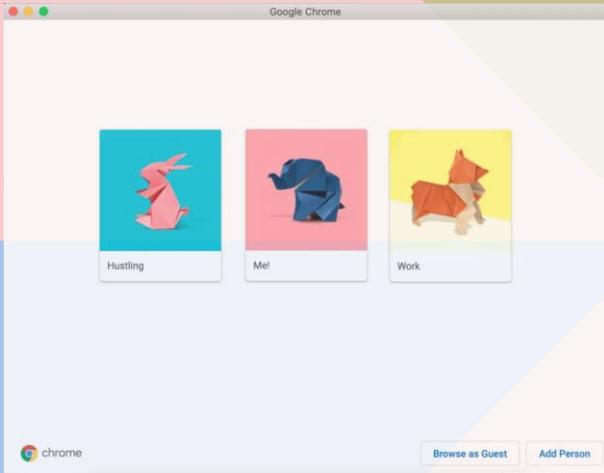
نصائح وارشادات عامة

- المراقبة المستمرة لموقعك، والإبلاغ مباشرة في حال وجود مشكلة أو تغيير في موقعك، فالكُل له دور في الحفاظ على الأمان، يجب الإبلاغ عن أي حالة غريبة أو مريبة داخل موقعك بدون خوف من لوم الآخرين وان لم يكن لك دخل في حدوثها، إذ يكون التركيز على تحديد المشاكل وحلّها بسرعة وكفاءة ثمّ البحث في كيفية تجنّب حدوثها مستقبلاً.
- يجب أن يكون استخدام كلمات مرور قوية يصعب تخمينها "يرفض WordPress أي تسلسل في الحروف أو الأرقام أو الرموز". استخدام كلمة مرور مختلفة لكل حساب أو خدمة وعدم استخدام كلمة المرور نفسها لحساباتك الشخصية وحسابات العمل. فاستخدام كلمات مرور مختلفة يضمن أنّه في حال عرف شخص ما كلمة مرور أحد الحسابات، لن يتمكّن من استخدامها لدخول حسابات أخرى. تأكّد أيضًا بضرورة عدم مشاركة كلماتك المرورية أو حساباتك مع الآخرين.



نصائح وارشادات عامة

- يفضل استخدام أجهزة محددة عند الدخول الى موقعك بصفة مدير، كأجهزة الحاسوب الشخصية أو الخاصة بتشكيلك، كما وتجنب استخدام أجهزة حاسوب مستخدمة لبرامج موكرة.
- ينصح باستخدام ملف شخصي "Profile" في متصفح الانترنت لكل حساب تمتلكه، وذلك لفصل الحساب الذي تستخدمه للدخول الى موقعك بصفة مدير عن الحسابات الأخرى.
- من المسائل الأمنية الشائعة التي يجب التنبيه لها هي التصيد الاحتيالي. التصيد الاحتيالي هو أسلوب يتبعه البعض لاستدراجك إلى مشاركة معلوماتك الشخصية على الإنترنت. ويتم ذلك عادةً باستخدام البريد الإلكتروني أو الإعلانات أو المواقع الإلكترونية المصممة لتبدو كأنها تابعة لأنشطة تجارية مشروعة تتعامل معها.



نصائح وارشادات عامة

7

- أخذ الحيطة والحذر عند النقر على مرفقات البريد الإلكتروني، أو تنزيل ملفات أو زيارة عناوين URL جديدة قد تكون مشبوهة أو تقدم خدمة مجانية. عدم النقر على الروابط المضمّنة في الرسائل الإلكترونية غير المرغوب فيها، والتنبّه لعنوان بريد المرسل الإلكتروني والتوقيعات.
- هناك خطوات أخرى يمكن اتّخاذها للحد من الهجمات على حساباتك مثل تفعيل ميزة "التحقّق بخطوتين". لا تقتصر هذه الميزة على إدخال كلمة المرور فحسب، بل عليك إجراء خطوة إضافية أيضًا للتمكّن من تسجيل الدخول، وتتمثّل الخطوة الثانية إمّا في إدخال رمز يتم إرساله إلى هاتفك أو في إدخال مفتاح أمان في جهاز الحاسوب. تُعدّ ميزة "التحقّق بخطوتين" طريقة فعّالة أيضًا للحد من التصيّد الاحتيالي.



(2FA) TWO-FACTOR AUTHENTICATION

two-factor authentication (2FA): المصادقة الثنائية وتسمى أيضاً two-step verification "التحقق بخطوتين" أو dual-factor authentication "المصادقة ثنائية العوامل"، وهي عملية أمان يوفر فيها المستخدمون عاملي مصادقة مختلفين للتحقق من أنفسهم، تُستخدم للتأكد من أن الأشخاص الذين يحاولون الوصول إلى حساب عبر الإنترنت، حيث يقوم المستخدم بإدخال اسم المستخدم وكلمة المرور الخاصة به. بعد ذلك، بدلاً من الوصول الفوري، سيطلب منهم تقديم معلومة أخرى.

تزيد المصادقة الثنائية من أمان حسابك. حتى إذا خمن شخص ما كلمة مرورك، فلن يتمكن من الوصول إلى حسابك.

كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)

The screenshot shows the WordPress dashboard interface. At the top right, the user profile menu is visible, containing the username 'alialjoboury', 'Edit Profile', and 'Log Out'. A red arrow with the number '1' points to the 'Edit Profile' option. Below the profile menu, there is a 'Quick Draft' section with fields for 'Title' and 'Content', and a 'Save Draft' button. To the left of the 'Quick Draft' section is the 'WP Mail SMTP' widget, which includes a 'View Detailed Email Stats' modal window and a 'Upgrade to WP Mail SMTP Pro' button. The dashboard also features a 'WordPress Events and News' section with a 'Select location' button and a message about upcoming events. At the bottom, there are statistics for 'All Emails' (3755 total, Sent N/A, Failed N/A) and a notification for 'NEW! Enable Weekly Email Summaries'.

كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)

The screenshot displays the WordPress admin dashboard. The top navigation bar includes 'My Sites', 'جامعة بغداد', '18', '+ New', 'Smart Slider', 'Theme Options', 'Purge cache', 'WP Mail SMTP', and 'Howdy, alialjoboury'. The left sidebar menu is open, with 'Users' selected. The main content area shows the 'Account Management' section, which includes 'New Password' (with a 'Set New Password' button), 'Sessions' (with a 'Log Out Everywhere Else' button), and 'Application Passwords' (with a 'Disabled' status and an 'Edit Wordfence Options' button). The 'Wordfence Login Security' section is visible, showing '2FA Status' as 'Inactive: Wordfence 2FA is inactive.' with a red arrow pointing to the 'Activate 2FA' button. The footer shows 'Version 6.0.3' and system information: 'جامعة بغداد • RAM 39.0/128M • SQL 205 • PHPv 7.4.27'.

كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)

My Sites جامعة بغداد 18 + New Smart Slider 1 Theme Options Purge cache WP Mail SMTP 1 Howdy, alialjoboury

Two-Factor Authentication

Two-Factor Authentication

[Learn more about Two-Factor Authentication](#)

Two-Factor Authentication, or 2FA, significantly improves login security for your website. Wordfence 2FA works with a number of TOTP-based apps like Google Authenticator, FreeOTP, and Authy. For a full list of tested TOTP-based apps, [click here](#).

- ### 1. Scan Code or Enter Key

Scan the code below with your authenticator app to add this account. Some authenticator apps also allow you to type in the text version instead.



ستظهر لك هذه الشاشة 3
- ### 2. Enter Code from Authenticator App

Download Recovery Codes *Optional*

Use one of these 5 codes to log in if you lose access to your authenticator device. Codes are 16 characters long plus optional spaces. Each one may be used only once.

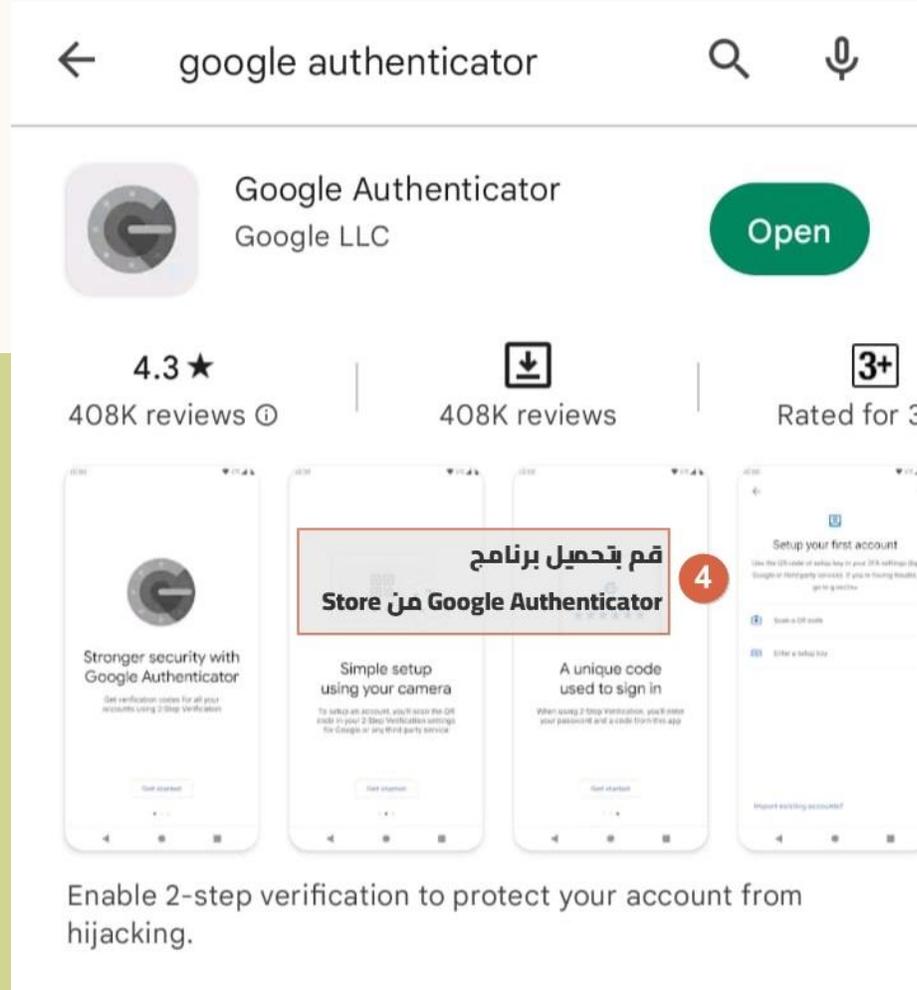
123456

Enter the code from your authenticator app below to verify and activate two-factor authentication for this account.

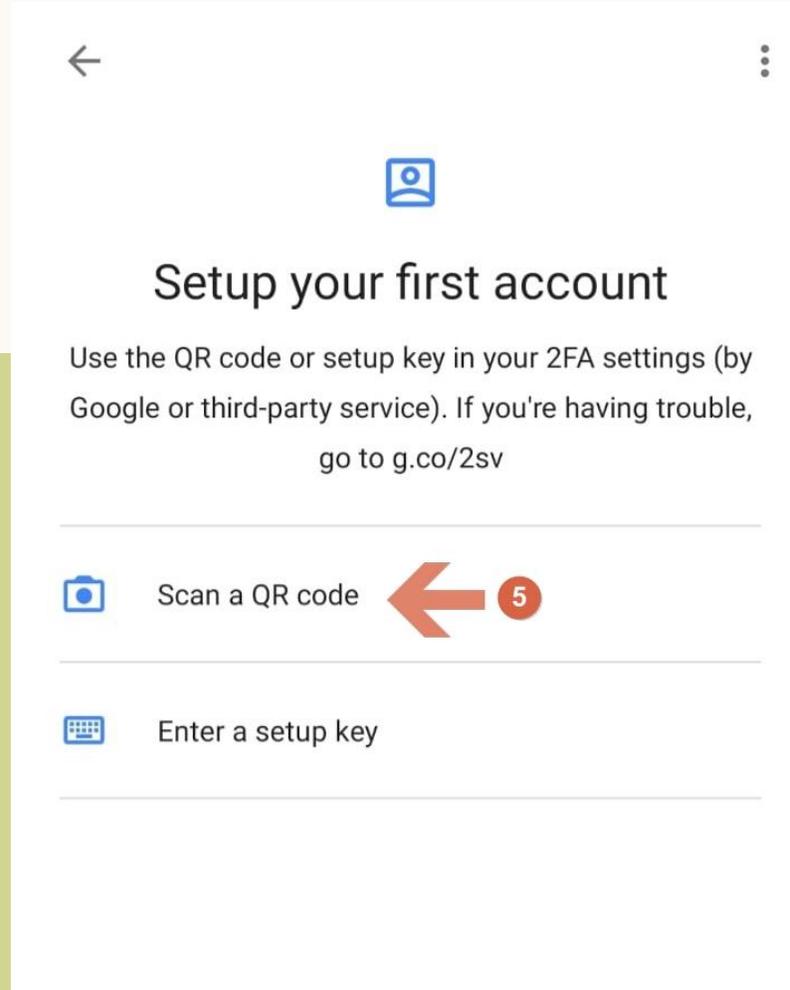
ACTIVATE

For help on setting up an app, visit our help article.

كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)



كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)



كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)

My Sites جامعة بغداد 18 + New Smart Slider Theme Options Purge cache WP Mail SMTP 1 Howdy, alialjoboury

Two-Factor Authentication

Learn more about Two-Factor Authentication

Two-Factor Authentication, or 2FA, significantly improves login security for your website. Wordfence 2FA works with a number of TOTP-based apps like Google Authenticator, FreeOTP, and Authy. For a full list of tested TOTP-based apps, [click here](#).

1. Scan Code or Enter Key

Scan the code below with your authenticator app to add this account. Some authenticator apps also allow you to type in the text version instead.



6

وجه كامرة هاتفك لمسح صورة الكود
2. Enter Code from Authenticator App

Download Recovery Codes *Optional*

Use one of these 5 codes to log in if you lose access to your authenticator device. Codes are 16 characters long plus optional spaces. Each one may be used only once.

4645 3453 9888 74x8
7194 5348 3764 4784
7649 4974 3453 5439
4234 3779 7234 7645
4325 4674 4474 4333

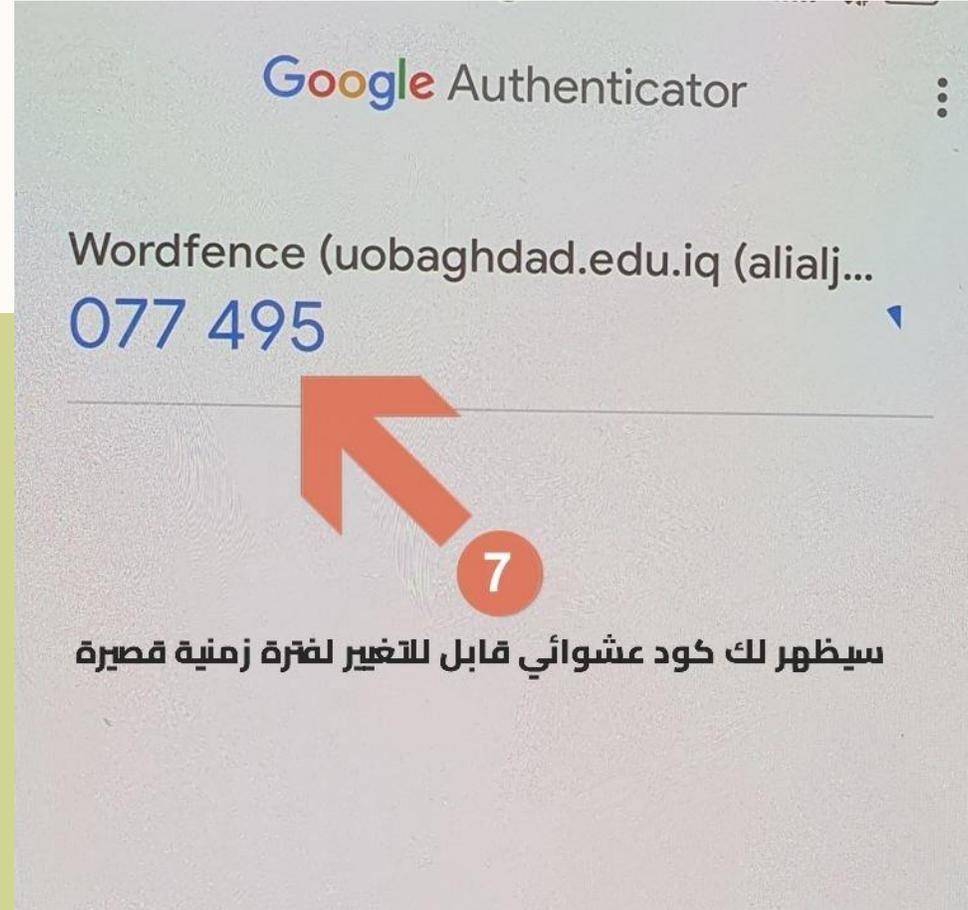
DOWNLOAD

Enter the code from your authenticator app below to verify and activate two-factor authentication for this account.

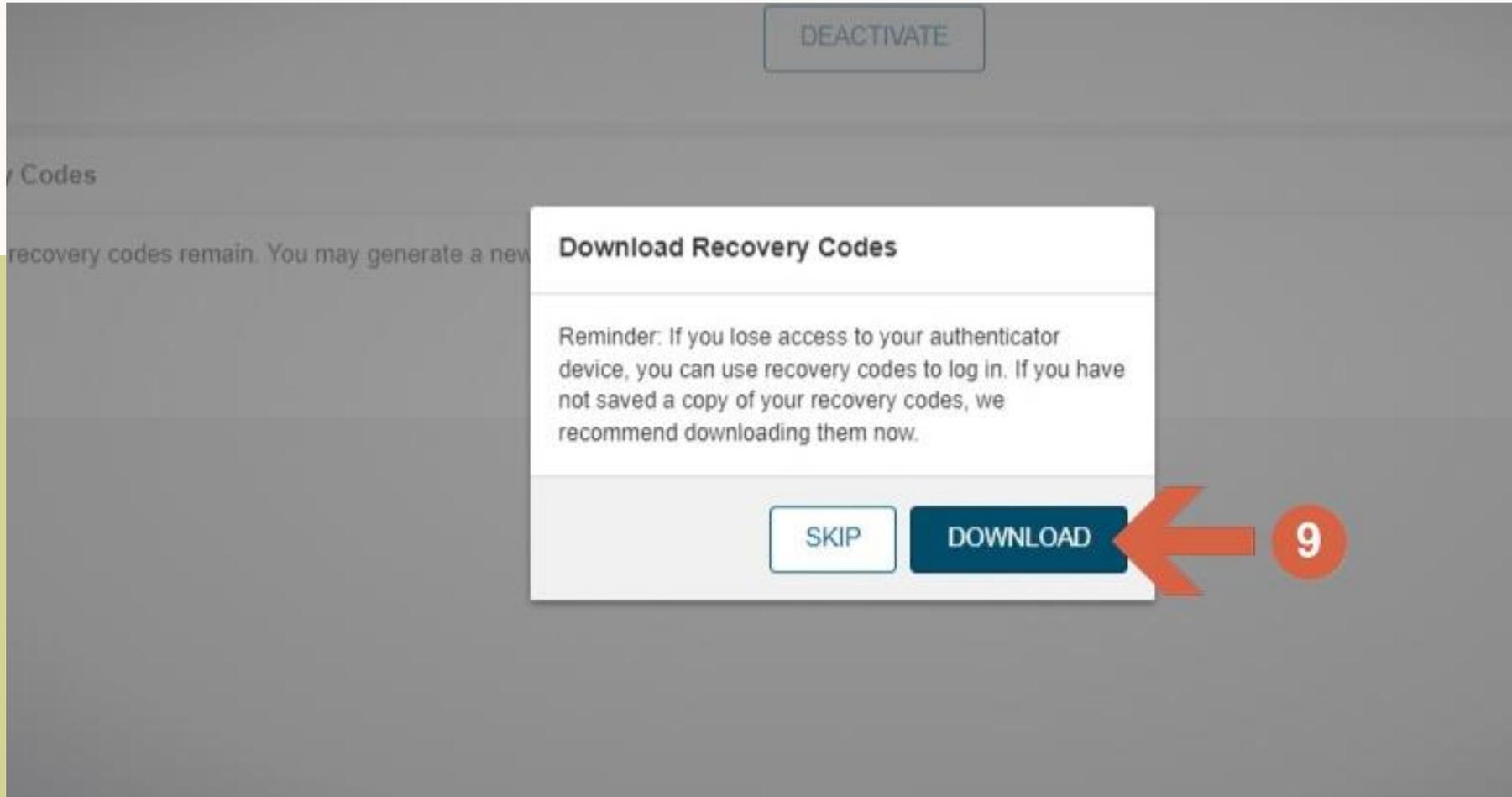
123456

ACTIVATE

كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)



كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)



كيف نفعّل 2FA لحسابات مواقعنا الإلكترونية في WORDPRESS (هذا الاجراء اجباري وليس اختياري)

اكتمل تفعيل 2FA

في كل مرة ستدخل لموقعك كمدير سيطلب منك اسم المرور وكلمة السر، ثم سيطلب رمز تحقق اضافي تحصل عليه من البرنامج المذكور سابقا

10

2FA Code

Log In

11

هل فقدت كلمة مرورك؟

→ الانتقال إلى جامعة بغداد

تغيير العربية

وشكراً لكم