ما الذي يمكنني القيام به للحفاظ على أمان حسابي على الفيسبوك؟

- **فكر قبل أن تضغط .** لا تضغط مطلقًا على الروابط الغريبة، حتى وإن كان مصدرها صديق تعرفه أو شركة تعرفها. (على سبيل المثال: روابط في الدردشة) أو في رسائل البريد الإلكتروني. إذا قام أحد أصدقائك بالضغط على رابط محتوى خبيث، فإنه يرسل لك هذا المنشور بشكل غير مقصود أو يقوم بالإشارة إليك في منشورات غير هامة. يجب أيضًا عدم تنزيل محتويات مثل: ملف بامتداد (exe. إذا لم تكن متأكدًا منه)
- **احذر من الصفحات والتطبيقات/الألعاب الزائفة.** يرجى الحذر من الصفحات التي تروّج لعروض جيدة للغاية يصعب أن تكون حقيقية. إذا كان لديك شك، فيرجى التحقق للتعرف على ما إذا كانت الصفحة قد تم التحقق منها .يرجى كذلك الانتباه عند تثبيت تطبيقات أو ألعاب جديدة. في بعض الأحيان، يستخدم المحتالون تطبيقات وألعاب سيئة للحصول على حق الوصول إلى حسابك على فيس بوك.
- **لا تقبل طلبات صداقة من أشخاص لا تعرفهم .**في بعض الأحيان، سيقوم المحتالون بإنشاء حسابات زائفة لارسال طلبات صداقة. وستسمح صداقتك مع المحتالين بأن يتمكنوا من الوصول لإرسال محتوى غير هام في يومياتك والإشارة إليك في المنشورات وإرسال رسائل ضارة إليك. كما قد ينتهي الأمر باستهداف أصدقائك الحقيقيين.
- **اختر كلمة سر فريدة وقوية .**استخدم مزيجًا من 8 أحرف وأرقام وعلامات ترقيم على الأقل ولا تستخدم كلمة السر هذه لأي من حساباتك الأخرى. يمكنك أيضًا استخدام كلمة سر آمنة مثلLastPass أو KeePass أو 1Password لتعيين وتذكر كلمات سر فريدة لحسابك.
- **لا تفصح عن معلومات تسجيل الدخول (مثل: عنوان البريد الإلكتروني وكلمة السر** .(في بعض الأوقات يعدك الأشخاص أو الصفحات بشيء ما (مثل: كروت شحن مجانية) إذا قمت بمشاركة معلومات حسابك معهم. إذا طلب منك إعادة إدخال كلمة السر الخاصة بك على فيس بوك (مثل: عند إجراء تغييرات على إعدادات الحساب لديك)، فتأكد من أن عنوان الصفحة لا يزال به **facebook.com/** في عنوان الويب وليس موقع وهمي اخر كمثال: facebook.hosting2.com.
- **تسجيل الدخول إلى موقع .www.facebook.com** في بعض الأحيان سيقوم المحتالون بإعداد صفحة زائفة لتبدو وكأنها صفحة لتسجيل الدخول إلى فيس بوك، آملين في أن تقوم بإدخال عنوان بريدك الإلكتروني وكلمة السر الخاصة بك. عليك التحقق من عنوان URL الخاص بالصفحة قبل إدخال معلومات تسجيل الدخول الخاصة بك. وإذا ساورتك الشكوك، فيمكنك دومًا كتابة **facebook.com** في المتصفح للعودة إلى موقع فيس بوك الحقيقي.
- **قم بتحديث المتصفح .**تحتوي أحدث إصدارات متصفحات الإنترنت على وظائف حماية أمان مضمنة. على سبيل المثال، قد تكون قادرة على تنبيهك إذا كنت على وشك الانتقال إلى موقع خداع مشبوه. اشهر المتصفحات وروابط تحديثها:
  - Mozilla Firefox
  - Safari
  - Google Chrome
  - Internet Explorer
- **تشغيل برنامج لمكافحة الفيروسات** .لحماية جهازك من الفيروسات والبرامج الضارة، قم بفحص الجهاز بحثًا عن فيروسات.

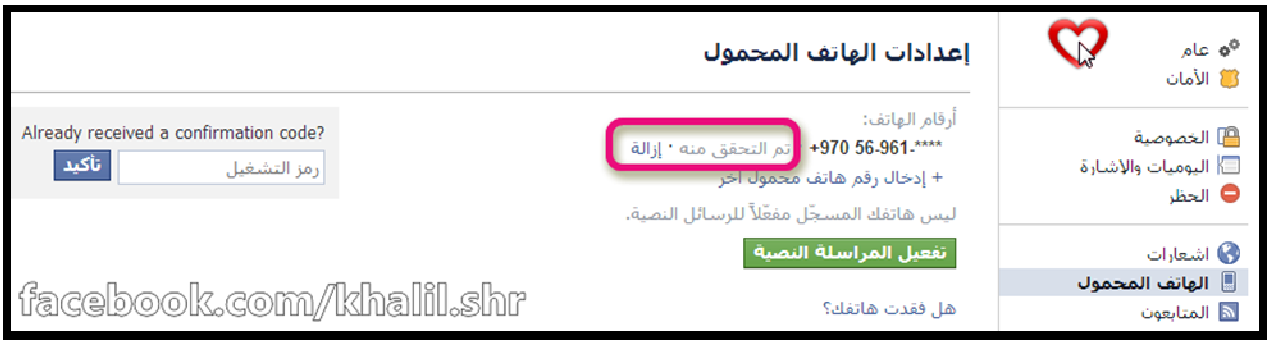
تتبع الخطوات التالية لحماية حسابك بشكل كامل :

1- **اضافة رقم هاتفك المحمول الشخصي .**

انقر على الرابط التالي لدخول صفحة اعدادات الهاتف المحمول :

https://www.facebook.com/settings?tab=mobile

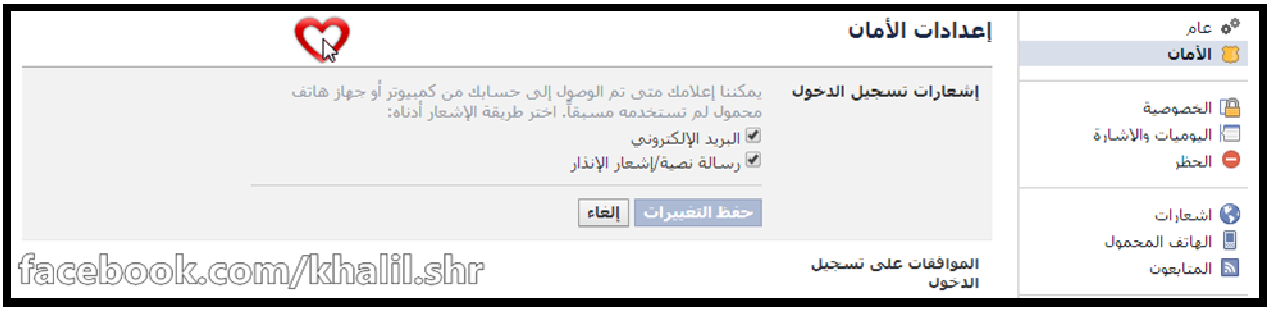
ومن ثم قم باضافة هاتفك المحمول، تأكد بان جملة " تم التحقق منه" موجودة .



2- **تفعيل اشعارات تسجيل الدخول .**

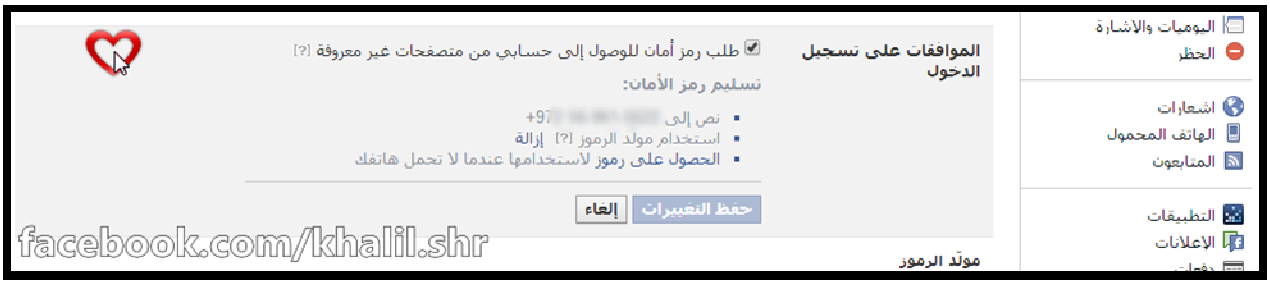
انقر على الرابط التالي لدخول صفحة اعدادات التنبيهات وقم بتفعيلها كما بالصورة :

https://www.facebook.com/settings?tab=security&section=notifications&view



3- تفعيل الموافقة على تسجيل الدخول ..

انقر على الرابط التالي لدخول صفحة اعدادات الموافقة على تسجيل الدخول وقم بتفعيل الخيار كما بالصورة :



4- اضافة جهات اتصال موثوق بها .

ما المقصود بجهات الاتصال الموثوق بها؟ كيف يمكنني إضافة جهات اتصال موثوق بها إلى حسابي؟

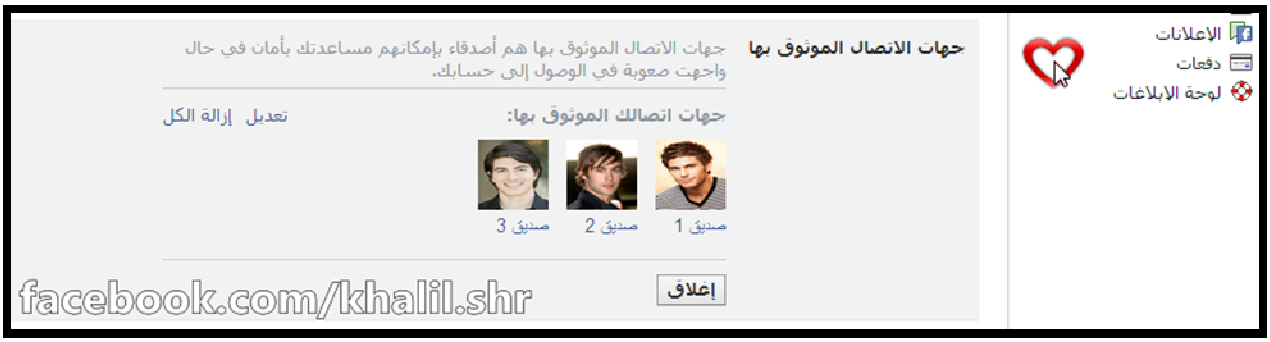
جهات الاتصال الموثوق بها هي الأصدقاء الذين يمكنك الوصول اليهم في حالة الحاجة إلى مساعدة لتسجيل الدخول إلى حسابك على فيس بوك (على سبيل المثال: إذا نسيت كلمة السر الخاصة بحساب فيس بوك ولا يمكنك تسجيل الدخول إلى حساب البريد الإلكتروني لإعادة تعيينها)

بعد إعداد جهات الاتصال الموثوق بها، ففي المرة القادمة التي يتعذر عليك فيها تسجيل الدخول إلى حسابك (قد يكون بسبب اختراق حسابك او نسيانك لبيانات تسجيل الدخول) يمكنك مطالبة فيس بوك بإرسال رموز الأمان الخاصة والتي تُستخدم لمرة واحدة إلى جهات اتصالك الموثق بها. ثم يمكنك بعد ذلك الاتصال بأصدقائك والحصول على الرموز لتسجيل الدخول إلى حسابك على فيس بوك.

لإضافة جهات اتصال موثوق بها لحسابك:

1. انتقل إلى الرابط التالي :
https://www.facebook.com/settings?tab=security&section=trusted_friends&view
2. اضغط على اختيار جهات الاتصال الموثوق بها
3. اختر من ثلاثة إلى خمسة أصدقاء وأكد اختياراتك

لتعديل أو إزالة جهات الاتصال الموثوق بها من حسابك، اتبع الخطوات من 1 إلى 3 ثم اضغط على تعديل بجوار جهات اتصالك الموثوق بها.



5- بعد التأكد من عمل كافة الخطوات السابقة , يمكنك الان حذف كافة المتصفحات الموثوقة التي قمت بتسجيل الدخول من خلالها. عند تسجيل الدخول على حساب الفيسبوك سوف يتم ارسال رسالة نصية تحتوي على رقم لهاتفك المحمول، بحيث تقوم بادخال هذا الرقم في المتصفح لتأكيد عملية تسجيل دخولك، حينها سوف يقوم الفيسبوك بمطالبتك لحفظ المتصفح كمتصفح موثوق به ام لا، اذا كان المتصفح على جهاز خاص بك تسخدمه انت فقط فيمكنك حفظ المتصفح حتى لا يتم مطالبتك برسالة نصية لهاتفك المحمول في عمليات تسجيل الدخول القادمة، اما في حاله كان المتصفح على جهاز نادرا ما تقوم التسجيل من خلاله او جهاز عام يستخدمه الاخرون فعليك عدم حفظ المتصفح.

حذف المتصفحات الموثوقه يزيد من حماية حسابك بحيث يتم المطالبة برقم لتاكيد هويتك وتسجيل دخولك من جديد.

من الملاحظ انه في حاله معرفة الاخرين لبيانات تسجيل دخولك الى حسابك، فانه من غير الممكن تسجيل الدخول طالما ان هاتفك المحمول ليس بحوزتهم، وبالتالي لن يستطيع احد معرفة الرسالة النصية التي تصل اليك ، ولكن هذا لا يعني ان تقوم بالافصاح للاخرين عن بياناتك الخاصة بشكل نهائي .

خليل شريتح

امن المعلومات – جامعة القدس المفتوحة

http://fb.com/khalil.shr

khalil@khalil-shreateh.com