مجلة قسم علوم الحاسوب

العدد الثالث

كلية علوم الحاسوب والرياضيات

جامعة الكوفة

إعداد:

م.مبرمج زهراء ازهر محمد

م.مبرمج اسيل فيصل عبد الواحد

م.مبرمج مروة عبد الله محمد

هل تُمثل طابعة جديدة من "إتش بي" نقلة نوعية للطباعة ثلاثية الأبعاد ؟

أطلقت "إتش بي "HP – مطلع الأسبوع الجاري طابعة جديدة ثلاثية الأبعاد تحمل الإسم .Metal Jet تستطيع الطابعة الجديدة، وهي لا تزال مُعدة حصرياً للإستخدام من قبل الشركات الكُبرى والمصانع وليس المُستخدم النهائي، طباعة نماذج ثلاثية الأبعاد مصنوعة من المعدن و ليس من المواد البلاستيكية المُعتادة في مجال الطباعة ثلاثية الابعاد حتى اليوم.

بالرغم من أن استخدامات إختبارية عديدة دخلت موضع التنفيذ مؤخراً، من بينها إستخدام الطباعة ثلاثية الأبعاد في تصميم المنازل وكذلك في تنفيذ أجزاء من قطع غيار السيارات، إلا أن طباعة هياكل معدنية لا تزال عقبة وتحدي كبير أمام الطباعة ثلاثية الأبعاد نظراً لصعوبة إستخدام المعدن كمادة خام يُمكن للطابعة ثلاثية الأبعاد تشكيلها وطباعتها.

يتم استخدام طابعة Metal Jet الجديدة تقنية جديدة كليا تُسمى binder-jet printing وهي فكرة ثورية طورتها الشركة وتقول عنها أنها ستجعل من طباعة المعادن ثلاثية الأبعاد واقعاً قابل للتطبيق. في الماضي، استخدمت بعض الشركات مفهوم الطباعة ثلاثية الأبعاد في تشكيل المعادن لصناعة بعض أجزاء الطائرات من خلال نحت كتلة كبيرة من المعدن بإستخدام الليزر في آلية تُشبه آلية تشكيل المعادن، ولكن طابعة HP الجديدة من خلال هذة التقنية تقوم فعلياً بطباعة المعدن بالشكل المطلوب من خلال رش رذاذ من ذرات المعدن في طبقات فوق بعضها البعض ومن ثم إضافة مادة لاصقة قوية تقوم بتثبيت هذا الرذاذ بالشكل المطلوب.

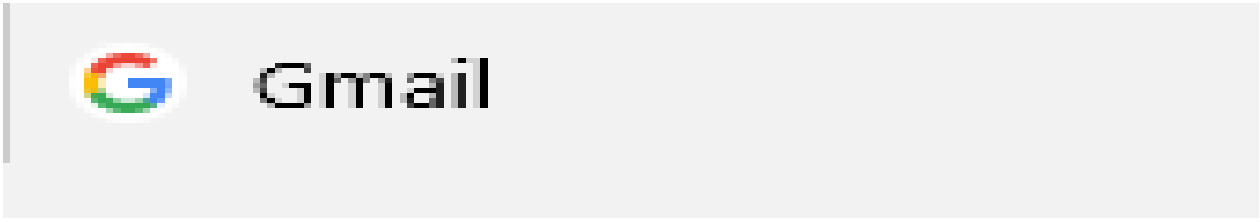
7 نقاط هامة لحماية صفحتك على الفيسبوك

الهدف من هذا الموضوع ان يعرف مدير كل صفحة كيف يمكن ان يتصرف سارق الصفحة ويبتعد عن الوقوع في خطأ ما يؤدي إلى سرقة صفحته.

حيث سنقوم بطرح عدة نقاط هامة وشبه شاملة لكي تضمن ان صفحتك في أمان وبعيداً عن لصوص الإنترنت

1- قم بحماية بريدك الإلكتروني :

في حال وصل السارق إلى بريدك الإلكتروني سيستطيع الوصول كافة حساباتك في المواقع وذلك عن طريق الضغط على زر (نسيت كلمة المرور) وسيقوم كل موقع بإرسال كلمة مرور جديدة إلى بريدك الالكتروني المخترق! لذلك ننصح باستخدام بريد ذو حماية جيدة مثل Gmail



2- لا تشارك كلمة سرك مع شخص آخر:

هذه المشكلة معروفة فالبعض يقوم بمشاركة كلمة السر مع شخص آخر (صديق او فرد من العائلة او شريك) وبعد فترة يحصل شجار قد يؤدي إلى انتقام عن طريق تغيير كلمة السر الخاصة بك

3- لا تقوم بالدخول إلى حسابك من جهاز آخر غير جهازك

فأغلب مقاهي الإنترنت يكون صاحب المقهى قادر على مشاهدة شاشتك كاملة وقد يكون يستخدم بعض البرامج لحفظ ما تقوم بكتابته على الكيبورد (ومن ضمنه كلمة سرك) كما يوجد عدة طرق اخرى لسرقة كلمة مرورك في حال استخدامك حاسوب شخص آخر

4- انتبه من الصفحات المزيفة :

أحياناً تقوم بالضغط على رابط فتظهر صفحة الفيسبوك بشكلها الطبيعي لتقوم بتسجيل دخولك ولكن هذه الصفحة قد تكون ليست للفيسبوك ولكنها تشبهها بشكل كبير او مثلها تماماً وهدفها هو سرقة كلمة مرورك فقط, تأكد ان رابط صفحة تسجيل الدخول مأخوذ من الموقع facebook.com و ليس facebook.website.com مثلاً

5- لا تقم بإضافة مدراء لا تملك ثقة كاملة بهم :

هذا الأمر شبيه بالنقطة الثانية إلى حد ما فمن الممكن ان يقوم الطرف الآخر بحذفك من قائمة المدراء في حال لم تكن تملك ثقة كاملة فيه, إضافة إلى احتمال ان تكون حمايته لحسابه ليست بالمستوى المطلوب ويقوم أحد ما بسرقة حسابه ومن ثم سرقة صفحتك

6- لا تقم بالضغط على روابط مشبوهة :

هذا الأمر هو الأقل خطراً, فمن المستحيل ان يتم سرقة حسابك بضغطة واحدة على رابط ما ولكن من الأفضل عدم الضغط مباشرة على الرابط, بل قم بنسخ الرابط وفتحه في متصفح آخر) لم تقم بتسجيل دخولك في حساب الفيسبوك الخاص بك) لتجربة ماذا سيفعل الرابط واين سيتم توجيهك

7- قم باستخدام متصفح آمن :

قم باستخدام متصفح آمن مثل Opera فالمتصفحات الأخرى مثل Internet Explorerو Firefox تقوم بحفظ كلمات السر بشكل مفضوح وهناك برامج سهلة جداً تستطيع كشف كلمات سرك المحفوظة على جهازك, اي في حال استطاع احد معارفك من الوصول إلى جهاز كمبيوترك لمدة ثواني معدودة سيستطيع سرقة كل كلمات سرك الذي قام المتصفح بحفظها,كما ان متصفح Google Chrome وFirfox يحوي خيار لعرض كلمات المرور المحفوظة بشكل مباشر وبدون تشفير

هذه هي النقاط الأساسية بشكل عام, وهي تغطي 95% من الأسباب التي تسببت بسرقة صفحات الفيسبوك

كيف تقوم بعمل نسخة احتياطية للنظام وطريقة استرجاعها

عملية أخذ نسخة احتياطية من ملفاتك جزء مهم في صيانة الكمبيوتر، لأن الجهاز معرض لكثير من الأخطار كالتلف أو دخول فيروسات وخاصة الأجهزة المحمولة. وفي ويندوز 7 يوجد أداة أساسية للنسخ الاحتياطي تمكنك من أخذ نسخة لملفاتك وحفظها في ذاكرة خارجية كأقراص DVD أو محرك أقراص خارجي أو على شبكة محلية خاصة بك.

لأخذ نسخة احتياطية من ملفاتك اتبع التالي:

1. **إذهب إلى "لوحة التحكم" Control Panel عن طريق زر "إبدأ" Start، ومن ثم "النظام والصيانة" System and Maintenance وبعد ذلك اختر "النسخ الاحتياطي والاستعادة" (Backup and Restore).**

. اضغط على "ضبط إعدادات النسخة الاحتياطية" Set up backup، وقد تستغرق النافذة التالية بعض الوقت لكي تظهر لك الأماكن المتاحة لحفظ النسخة.

. إختر مكان الحفظ؛ كما سبق وذكرنا يمكنك استعمال ذاكرة خارجة أو DVD أو على الجهاز نفسه لكن على قرص آخر، وفي حال قمت بعمل نسخة للنظام ككل سيتطلب ذلك مساحة أكثر من 10 جيجابايت، أما إن اخترت بعض الملفات كالمستندات والصور فلن يتطلب ذلك الكثير من المساحة.
. تابع للخطوة التالية واختر منها نوع الحفظ تلقائي أم مخصص، بحيث يختار الحفظ التلقائي الملفات الموجودة في المستندات وسطح المكتب ليتم نسخها، أما في خيار الحفظ المخصص يمكنك اختيار الملفات المراد أخذ نسخة منها ويخيرك إن أردت عمل نسخة من النظام أيضًا.
. يمكنك اختيار الجدولة للنسخ الاحتياطي وتحديده بتوقيت معين يوميًا أو أسبوعيًا أو شهريًا.

ستبدأ عملية النسخ الاحتياطي بعد ذلك، ومن الأفضل أن تترك الجهاز حتى تنتهي العملية التي ستستغرق بعض الوقت في المرة الأولى. احفظ النسخة الاحتياطية في مكان آمن، ويمكنك استرجاعها في أي وقت أردت ذلك عن طريق:

. إعادة إقلاع الجهاز وأثناء الاقلاع يتوجب الضغط على زر F8 للدخول إلى خيار صيانة النظام.
. ومن داخل الخيار قم باختيار اللغة التي تريد أو اضغط OK للاختصار.
. تظهر نافذة بأسماء مستخدمي الجهاز، اختر الحساب المسؤول وأدخل كلمة المرور إن وجدت.
. تظهر عدة خيارات، نختار منها System Image Recovery.
. انتظر بعض الوقت ليتعرف على مكان النسخة الاحتياطية.

- **إذا كانت في الجهاز نفسه سيتعرف عليها تلقائيًا، وإن كانت على قرص خارجي يجب أن يكون موصولًا بالجهاز ومن ثم تحديده.**
- **قم بالموافقة لتبدأ عملية استعادة الملفات من النسخة الاحتياطية التي عملتها سابقًا.**

بذلك تكون قد أعدت ملفاتك وخصائص حسابك دون أي ضياع، وبطريقة بسيطة مدمجة مع نظام تشغيل ويندوز بشكلٍ أساسي.