معلومات عن الاستخدام عند التداول عبر الإنترنت

١. تجنب دخول حساب التوفيق تداول الخاص بك من مقاهي الإنترنت أو الحاسب الآلي المشترك .على أية حال ، إذا أردت القيام بذلك قم بتغيير كلمات مرورك من حاسبك الآلي الخاص .

٢. في كل مرة تكمل فيها جلستك للتداول الإلكترونية ، سجل الخروج من www.afg-sa.comأولا ثم أغلق المتصفح الخاص بك .

٣. للدخول للتداول الإلكتروني ، أكتب دائماً في معرف الموارد الموحد الصحيح www.afg-sa.comفي نافذة المتصفح. لا تنقر أبداً على الرابط الذي يقدم لأخذك إلى موقعنا .

٤. غير كلمات مرور تجارتك الإلكترونية بشكل منتظم (مرة على الأقل في الشهر)

٥. ينبغي أن تكون كلمة مرورك معقدة وصعبة لكي لا يمكن تخمينها من قبل الآخرين . استخدم الحروف ، الأرقام والرموز الخاصة مثل [(,) * &, ^, %, $, #, @, !] في كلمات مرورك .

٦. إذا كانت لديك أكثر من بطاقة مستخدم واحدة للتداول الإلكترونية ، استخدم كلمة مرور مختلفة عن كل بطاقة مستخدم .

٧. لا تشارك أبداً كلمات مرور تجارتك الإلكترونية مع الآخرين ، حتى مع أفراد العائلة. لا تفصح عنها لأي شخص ، حتى موظف مجموعة التوفيق المالية .

٨. استخدم البرمجيات المضادة للفيروسات، أهم شيء يمكن لك القيام به لحماية حسابك ومعلوماتك الشخصية هو تشغيل الإصدار الأخير لبرنامج البرمجيات المجرب ضد الفيروسات على حاسبك الآلي. سوف تساعدك البرمجيات المضادة للفيروسات على حماية نظامك من برامج " حصان طروادة " ، التي يمكن إرسالها لك عبر البريد الإلكتروني .يمكن لبرامج حصان طروادة استلام وإرسال أية معلومات موجودة على نظامك ، بما فيها كلمات المرور الخاصة بك دون موافقتك .

٩. استخدام حزمة جدار النار الشخصية، أي حاسب آلي أو جهاز متصل مع الإنترنت وغير المحمي كما ينبغي عرضة لمجموعة من الاقتحامات والهجمات الماكرة للإنترنت .ينطبق ذلك على جميع مستخدمي مودمات الكبل ، خطوط الاشتراك الرقمية وخطوط الاتصال .لكن ، مستخدمي مودم الكبل وخطوط الاشتراك الرقمية يكونون بخاصة عرضة للخطر لأن كلتا طريقتي التوصيل توفر " القدرة على التوصل دائماً ". إن احتمال وجود شخص ماكر يدخل على حاسبك الآلي يزيد من بقاء حاسبك في وضع تشغيل لفترة أطول ومتصل مع الإنترنت .وسوف يساعدك جدار النار الشخصي على حمايتك من الاقتحام. تنشيء جدار النار الحاجز بين حاسبك الآلي وبقية الإنترنت. يمكن أن يكون جدار النار جهاز عُـدد ، تطبيق برمجيات أو مجموعة مؤتلفة من كليهما. يمكن أن تمنع جدران النار الهجمات الماكرة وسد أنواع معينة من البيانات من دخولها على حاسبك الآلي أو الشبكة الخاصة. يمكن أيضاً ضبطها لإيقاظك وتنبيهك إذا حاول أي شخص من الدخول إلى نظامك .

١٠. استخدام حاسبك الآلي، يمكن أن تسرق كلمات المرور حينما تسجل الدخول في موقع الويب بإستخدام كمبيوتر شخص آخر ، مثل ردهة الفندق ، المطعم ، أو المطار. قد تكون لهذه الحاسبات الآلية برامج حصان طروادة عليها والتي سوف تعترض كل ضربة مفتاح تدخلها ، بما فيها كلمات المرور الخاصة بك ، وإرسالها إلى أي شخص محتمل في أي مكان في العالم .

١١. قم بتحديث مستعرضك ونظام تشغيلك بمحدثات البرمجيات، إن البرمجيات التي تستخدمها والإنترنت ذاته يمكن أن تؤثر على النشرات الأمنية التي تحذرك عن الثقوب أو العلل الأمنية المختلفة التي قد تؤثر على البرمجيات ومستعرض الويب الذي تستخدمه .ومن الأهمية بمكان مراجعة مواقع شبكة نظام تشغيلك وبائعي مستعرض الويب لمجموعات البرمجيات والتحديثات. يمكن تهيئة بعض نظم التشغيل والبرمجيات لتراجع تلقائياً التحديثات الجديدة .

١٢. تنشيط الحاجز المنبثق، إن العديد من البرامج الحرة والمتاحة عموماً الموجودة سوف تعترض جميع النوافذ المنبثقة من الحدوث بينما تكون على الخط. بإمكانك تحميل تلك البرامج من الإنترنت .

١٣. قم بعمل المسح الضوئي لحاسبك الآلي بسبب أدوات التجسس بشكل منتظم، أدوات التجسس وأدوات الإعلان هي البرامج التي تراقب نشاط الإنترنت لديك وترحل المعلومات إلى مصدر قابل للتوزيع. البرامج الخالية من أدوات التجسس ـ الإزالة متوفرة على الإنترنت .