

پاسخ اولین پرسش : خیر این فایل هیچ ربطی به اینترنت اکسپلورر ندارد

پوشه AppData مکان ایده‌آلی برای مخفی کردن برنامه‌های مخرب است. باید به هر برنامه‌ای که در این پوشه است دقت کرد. جای اینترنت اکسپلورر به هیچوجه در این پوشه نیست. اگر فایل اجرایی اینترنت اکسپلورر در این پوشه باشد، کلیک کردن روی آن ریسک بزرگی است چون بطور طبیعی فایل اجرایی اینترنت اکسپلورر در Program Files است. ایکن هر برنامه‌ای همینطور نام و حجم آنرا میتوان تغییر داد. این موضوع مهمی است که باید همیشه بخاطر داشته باشید.

پاسخ دومین پرسش : خیر این یک سایت جعلی است که برای هک کاربران فیسبوک است

سایتهای جعلی از این دست که مخرب هستند میتواند در ابتدای ادرس خود قفلی سبز رنگ داشته و با HTTPS آغاز شوند اما دقت کاربر برای بدام نیفتادن نیز اهمیت بسیار دارد و با کمی وقت متوجه میشوید که کلمه فیسبوک بجای حرف اف با حرف ال نوشته شده و در نتیجه یک سایت شبیه سازی شده و یا جعلی فیسبوک میباشد.

پاسخ سومین پرسش : با خود میگوئید که این یک هشدار جعلی است و آنرا نادیده میگیرید.

بعضی انتی ویروسهای جعلی به کاربران وانمود میکنند که روی کامپیوتر آنها برنامه مخربی یافته اند. در صورتیکه با خیال حذف این برنامه‌های مخرب خیالی روی دکمه Remove کلیک شود پیام دیگری نمایش داده شده و از کاربر خواسته میشود تا برای حذف ویروس و یا ویروسهای یافت شده این برنامه جعلی را خریداری کند.

پاسخ چهارمین پرسش : *2+M۴F-tA۶

هر چند که تعداد کاراکترهای یک رمز عبور مهم است اما مشکل بودن رمز عبور و استفاده از کاراکترهای متفاوت چون حروف بزرگ و کوچک و اعداد و کاراکترهای مخصوص نیز بسیار اهمیت دارد. یک رمز عبور طولانی که فقط از اعداد و یا فقط از حروف تشکیل شده قابل اعتماد نیست.

پاسخ پنجمین پرسش : ۱۲۳

در ابتدا باید الودگی کامپیوتر را از بین برده و سپس رمز عبور و یا رمز عبورهای خود را تغییر داد چون تغییر دادن آنها در حالیکه هنوز برنامه‌های مخربی روی کامپیوتر هستند بی فایده است.

پاسخ ششمین پرسش : WPA ۲

پاسخ "نمیدانم" به این پرسش همانقدر اهمیت دارد که از پروتکل WEP استفاده شود. ناگاهای یکی از نقاط ضعف مورد علاقه هکرها است و هر کاربری باید روشهای امنیتی برای محافظت از دستگاه خود را بداند تا خطر هک شد خود را کاهش دهد.

پاسخ هفتمین پرسش : خیر. هرگز.

ارسال رمز عبور میتواند امکان اینترسپت انرا از طریق شبکه فراهم سازد و بعلاوه ایا واقعا مطمئن هستید که هکری با هک ایمیل یکی از نزدیکان شما پیامی برای پرسیدن رمز عبورتان ارسال نکرده باشد؟ هیچ وقت نباید جانب احتیاط را از دست داد و ارسال رمز عبور با ایمیل توصیه نمیشود. میتوانید احيانا رمز عبور خود را در صورتی که حتما نیاز است که به یکی از نزدیکان بگوئید حضورا به او بگوئد و مسلما بعدا نیز نباید فراموش کنید که انرا تغییر دهید.

پاسخ هشتمین پرسش : موضوعی است که باید انرا جدی گرفت

در اینکه در درجه اول امنیت انفورماتیک کاری است که به عهده متخصصینی است که باید امنیت ما را محافظت کنند شکی نیست اما هر کسی باید حداقل آشنائی با امنیت انفورماتیک برای ایمن ساختن دستگاه خود را نیز داشته باشد.

پاسخ نهمین پرسش : برای هر سایت رمز عبوری مخصوص ان سایت دارم و هر چند گاه نیز انرا تغییر میدهم

لزومی ندارد که هر روزه و یا هر هفته رمز عبورهای خود را تغییر دهید اما تغییر گاه بگاه آنها امنیتی بیشتر است و بخصوص توصیه نمیشود که از یک رمز عبور برای همه سایتها استفاده شود چون در صورتی که هکری پسورد یک اکانت کاربری را بدست ارد مسلما کار هکر راحت تر شده و به همه اکانتهای شما میتواند دسترسی پیدا کند.

پاسخ دهمین پرسش : حساب بانکی میتواند با یک برنامه هک و فقط یک کلیک هک شود

روشهای بسیاری برای هک وجود دارند اما نرم افزاری که با ان بتوان فقط با یک کلیک یک حساب بانکی را هک کرد وجود ندارد.