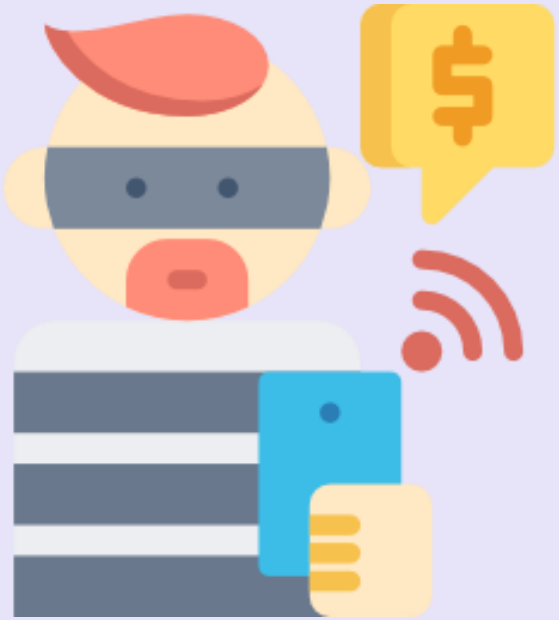
نکات امنیتی استفاده از شبکه های اجتماعی

پلیس فضای تولید و تبادل اطلاعات ناجا

۱ در مورد هویت افراد در شبکه های اجتماعی، بیشتر دقت کنید.

ممکن است سارقان هویت به منظور دریافت اطلاعات شما، پروفایل های جعلی ایجاد کنند. افراد همیشه آن چیزی که می گویند، نیستند.



۲ رعایت احتیاط در مورد کلیک کردن بر روی لینک ها

حتی اگر لینک در پیامی است که از سوی دوست شما فرستاده شده است در هنگام کلیک کردن بر روی آن با احتیاط باشید. به این علت که ممکن است اطلاعات حساب کاربری دوست شما سرقت شده باشد و با استفاده از آن در حال ارسال لینک های مخرب به لیست تماس های او باشند.

۳ در مورد اطلاعات شخصی که منتشر می کنید، مراقب و محتاط باشید.

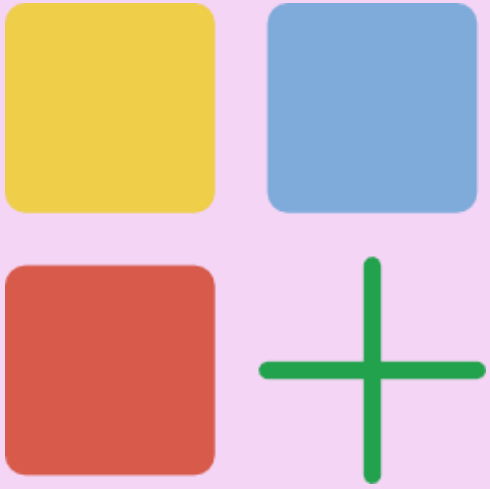
یک راه معمول مجرمان سایبری برای نفوذ به حساب کاربری شما بوسیله کلیک کردن بر روی لینک "رمز عبور خود را فراموش کرده اید؟" می باشد. با پاسخ به سوال امنیتی می تواند به درون حساب کاربری راه یابد. مجرمان سایبری سعی می کنند پاسخ این سوالات را در پروفایل شخصی و یا در پُست هایی که فرد در صفحه شبکه اجتماعی قرار می دهد، پیدا کنند. در نتیجه اگر شما اطلاعات بیشتری را در پروفایل و یا صفحه خود ارائه کرده باشید کار را برای هکر جهت پیدا کردن جواب سوال های امنیتی و نفوذ به حساب کاربری راحت تر کرده اید.

٤ آدرس سایت شبکه اجتماعی را به طور مستقیم در مرورگر تایپ نمایید.

اگر شما بر روی لینکی کلیک کنید که شما را به سمت وب سایت شبکه های اجتماعی از طریق یک ایمیل یا دیگر وب سایت ها هدایت کند. ممکن است در حقیقت آن یک مورد فیشینگ باشد که سایت اصلی را جعل کرده است و کاملا شبیه به سایت اصلی به منظور فریب کاربران طراحی شده است تا کلمات عبور و رمز آن ها را بدست آورد.

۵ مراقب برنامه های جانبی که نصب می کنید، باشید.

بسیاری از سایت های شبکه های اجتماعی به شما اجازه دانلود برنامه های جانبی را می دهند که شما می توانید از طریق آن ها کارهای بیشتری را در صفحات شخصی خود انجام دهید. با این حال، مجرمان سایبری می توانند از این برنامه های جانبی برای سرقت اطلاعات افراد استفاده کنند بدون آن که فرد متوجه شود.



٦ هر آنچه که شما ارسال می کنید، دائمی است.

این را بدانید که هر اطلاعاتی که شما در شبکه های اجتماعی ارسال می کنید دائمی است. قبل از آن که هر مطلبی را ارسال کنید به خوبی در مورد آن فکر کنید.

۷ تنظیمات حریم خصوصی را جدی بگیرید.

از تنظیمات حریم خصوصی به منظور اینکه، بتوانید کنترل کنید چه کسانی اطلاعات شخصی شما را مشاهده می نمایند، استفاده کنید.

سیاست های حریم خصوصی سایت و شبکه اجتماعی را که از آن استفاده می کنید، مطالعه نمایید و بدانید که آن شبکه اجتماعی از اطلاعات شما چه استفاده هایی می کند.

۸ هرگز از رمز های یکسان برای چند حساب کاربری استفاده نکنید.

این مسئله فقط مربوط به شبکه های اجتماعی نیست، بلکه برای تمامی حساب ها باید این امر رعایت شود. رعایت این مسئله باعث می شود، در صورتی که به یکی از حساب های شما نفوذ شود،حساب دیگر در معرض خطر قرار نگیرد.

۹ استفاده از شبکه های اجتماعی در محل کار، کار درستی نیست.

دسترسی به سایت های شبکه های اجتماعی در محل کار از طریق سیستم ها و کامپیوترهای محل کار شما را با ریسک حملات ویروسی مواجه می کند. برای مثال، با باز کردن پیوست یک ایمیل و یا با کلیک کردن بر روی لینک دانلود یک برنامه، کامپیوتر محل کار شما می تواند آلوده به بد افزارها و برنامه های مخرب شود و اطلاعات مورد سرقت قرار گیرد.

همیشه به یاد داشته باشید:

امنیت یک محصول نیست، یک فرآیند است.

منبع: ایران هشدار