

گاهنامه آگاهی رسانی امنیت سایبری

محافظت آنلاین



در عصر دیجیتال امروزی، شبکه‌های اجتماعی و استفاده از اینترنت هم برای شغل حرفه‌ای و هم زندگی شخصی ضروری است. با این حال، این سکوها در صورت عدم استفاده ایمن، خطرات امنیتی قابل توجهی را نیز به همراه خواهند داشت. در اینجا نکات کلیدی برای محافظت از خود و شرکت در حین گشت‌وگذار در دنیای آنلاین آورده شده است:

۱. در مورد اطلاعات شخصی محتاط باشید:

◀ **اشتراک‌گذاری محدود:** از به اشتراک‌گذاری اطلاعات حساس شخصی یا شرکتی (مانند عنوان شغل، مکان یا پروژه‌های داخلی) در پلتفرم‌های رسانه‌های اجتماعی خودداری کنید.



◀ **تنظیمات حریم خصوصی:** به‌طور منظم تنظیمات حریم خصوصی خود را بررسی و به‌روز کنید تا کنترل کنید چه کسی می‌تواند پست‌ها و اطلاعات شخصی شما را ببیند.



۲. مراقب کلاهبرداری‌های فیشینگ باشید:

◀ **حملات فیشینگ:** در شبکه‌های اجتماعی بسیار رایج است و می‌تواند به‌صورت پیام‌های مستقیم یا پیوند در پست‌ها، رایانه شما را آلوده کند.



◀ **روی لینک‌های مشکوک کلیک نکنید:** مراقب پیام‌های ناخواسته یا درخواست‌های افراد ناشناس باشید. کلاهبرداران اغلب به‌عنوان دوستان یا همکاران ظاهر می‌شوند تا شما را فریب دهند تا روی پیوندهای مخرب کلیک کنید.



۳. از رمزهای عبور قوی و منحصر به فرد استفاده کنید:

اطمینان حاصل کنید که هر حساب شبکه‌های اجتماعی و اینترنت از یک رمز عبور منحصر به فرد و پیچیده استفاده می‌کند. برای افزودن یک لایه امنیتی اضافی، احراز هویت چندعاملی (MFA) را در همه حساب‌ها فعال کنید.



۴. مراقب برنامه‌های شخص ثالث باشید:



از دادن مجوزهای غیرضروری به برنامه‌های متفرقه متصل به حساب‌های رسانه‌های اجتماعی خود اجتناب کنید. این برنامه‌ها می‌توانند به صدا، تصویر و مکان شما دسترسی داشته باشند و خطرات امنیتی ایجاد کنند. فقط از برنامه‌های منابع قابل اعتماد استفاده کنید و به‌طور مرتب بررسی کنید که کدام برنامه‌ها به حساب‌های شما دسترسی دارند.

۵. محافظت در برابر مهندسی اجتماعی:



مهندسی اجتماعی فریب افراد برای افشای اطلاعات محرمانه است. مهاجمان ممکن است از شبکه‌های اجتماعی برای جمع‌آوری جزئیات درباره شما یا سازمانتان استفاده کنند. مراقب آنچه به اشتراک می‌گذارید باشید و از پاسخ به پیام‌های مشکوک که اطلاعات حساس را درخواست می‌کنند، خودداری کنید.

۶. مرور اینترنت خود را ایمن کنید:



◀ **از HTTPS استفاده کنید:** همیشه مطمئن شوید که وبسایت‌هایی که بازدید می‌کنید از HTTPS استفاده می‌کنند (به دنبال قفل در نوار آدرس مرورگر بگردید) تا مطمئن شوید اتصال شما ایمن است.



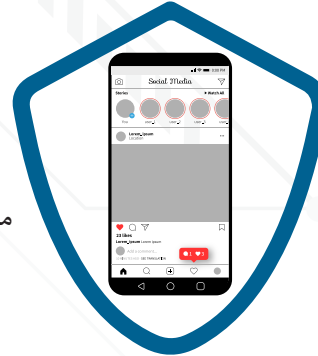
◀ **اجتناب از وای فای عمومی:** هنگام دسترسی به اطلاعات حساس، از استفاده از شبکه‌های وای فای عمومی خودداری کنید. در صورت لزوم، همیشه از VPN برای رمزگذاری اتصال خود استفاده کنید.

۷. قبل از ارسال، فکر کنید:

◀ **امنیت شخصی:** از ارسال به روزرسانی‌های بی‌درنگ درباره مکان، برنامه‌های سفر یا سایر جزئیات شخصی خود که می‌تواند توسط مجرمان سایبری مورد سوءاستفاده قرار گیرد، خودداری کنید.



◀ **امنیت شغلی:** از ارسال پست در مورد فعالیت‌های کاری حساس یا اطلاعات محرمانه شرکت خودداری کنید. حتی جزئیات به ظاهر بی‌ضرر در مورد شغل شما می‌تواند در حملات هدفمند استفاده شود.



۸. به‌طور منظم بر حساب‌های خود نظارت کنید:

مکرر رسانه‌های اجتماعی و حساب‌های آنلاین خود را برای هرگونه فعالیت مشکوک یا دسترسی غیرمجاز زیر نظر بگیرید. گونه رفتار غیرعادی، مانند تلاش‌های ناشناخته برای ورود به سیستم یا تغییرات در تنظیمات حساب خود، فوراً به پلتفرم یا مدیریت فناوری اطلاعات خود گزارش دهید.



۹. از مرورگرهای امن و موتورهای جستجو استفاده کنید:

از مرورگرهایی استفاده کنید که امنیت و حریم خصوصی را در اولویت قرار می‌دهند و ویژگی‌هایی مانند مسدودکننده‌های تبلیغات و ابزارهای ضد ردیابی را فعال می‌کنند تا قرار گرفتن در معرض تهدیدات آنلاین را به حداقل برسانند.



شبکه های اجتماعی محبوب در ایران از سهولت تا امنیت چاقوی دو طرفه

شبکه های اجتماعی در ایران برای ارتباط افراد فردی یا گروهی و به اشتراک گذاری اطلاعات به طور گسترده مورد استفاده قرار می گیرند. با این حال، بسیاری از این پلتفرم ها با خطرات امنیتی و حریم خصوصی قابل توجهی همراه هستند.

شبکه های اجتماعی پرطرفدار در ایران:

اینستاگرام:

یک پلتفرم پیشرو برای به اشتراک گذاری عکس و ویدیو، که به طور گسترده برای استفاده شخصی و کسب و کار آنلاین مورد استفاده قرار گرفته است.



تلگرام:

یکی از پرکاربردترین اپلیکیشن های پیام رسان در ایران که از دیرباز محبوبیت دارد.



آپارات:

یک پلتفرم ایرانی اشتراک گذاری ویدیو، که اغلب به عنوان نسخه ایرانی یوتیوب شناخته می شود.



WhatsApp:

یکی از اپلیکیشن های پیام رسان که بیشتر برای ارتباطات خصوصی و گروهی مورد استفاده قرار می گیرد.



رویکا:

اپلیکیشن پیام رسان جهت خدمات ویدیویی و شبکه های اجتماعی را ارائه می دهد.



خطرات حریم خصوصی:

بسیاری از شبکه های اجتماعی داده های حساس کاربران را جمع آوری و ذخیره می کنند که ممکن است در معرض سرقت داده ها قرار بگیرند.

پلتفرم های خارجی (به عنوان مثال تلگرام، اینستاگرام و واتس آپ) حفاظت از حریم خصوصی ضعیفتری داشته دارند و تحت نظارت دولت خارجی و حتی کلاهبرداران می باشند. به همین دلیل با تلاش متخصصان ایرانی و با حمایت گسترده مردم استفاده از شبکه های اجتماعی ایرانی با افزایش بی سابقه ای داشته است.



اکانت های جعلی و کلاهبرداری:

پلتفرم هایی مانند اینستاگرام و تلگرام مملو از حساب های جعلی، کلاهبرداری های فیشینگ و لینک های تقلبی هستند.

حملات فیشینگ:

کاربران تلگرام و واتس اپ اغلب با پیام های فیشینگ حاوی لینک های مخرب یا صفحات لاگین جعلی هدف قرار می گیرند.



هک حساب کاربری:

بسیاری از کاربران به دلیل گذرواژه های ضعیف، عدم احراز هویت دو مرحله ای (۲FA) یا کلیک بر روی لینک های مخرب قربانی هک حساب می شوند.

اشتراک گذاری بیش از حد محتوا:

به اشتراک گذاری بیش از حد اطلاعات شخصی، داده های مربوط به کار یا مکان ها در پلتفرم هایی مانند اینستاگرام یا تلگرام می تواند افراد و سازمان ها را در معرض حملات هدفمند قرار دهد.



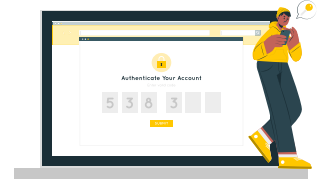
خطرات VPN و پروکسی:

دسترسی به پلتفرم های محدود شده (مثلاً توییتر، لینکدین) اغلب به VPN نیاز دارد، که ممکن است همیشه اتصالات امنی را فراهم نکند و کاربران را در معرض حملات مردی در میان قرار دهد.

بهترین روش ها برای ایمن ماندن در شبکه های اجتماعی:

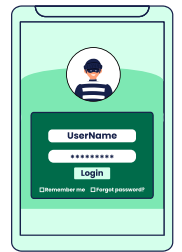
احراز هویت دو مرحله ای (۲FA):

با فعال سازی این قابلیت از حساب های کاربری خود در تمامی شبکه های اجتماعی محافظت کنید.



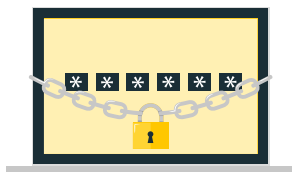
از اشتراک گذاری بیش از حد خودداری کنید:

در مورد ارسال اطلاعات شخصی یا کاری به صورت آنلاین محتاط باشید.



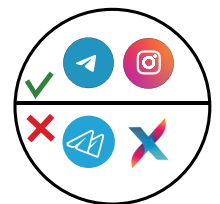
تأیید پیوندها و حساب ها:

روی پیوندهای مشکوک کلیک نکنید و با حساب های ناشناس تعامل نکنید.



از گذرواژه های قوی استفاده کنید:

حساب های خود را با گذرواژه های منحصر به فرد و پیچیده ایمن کنید.



به برنامه های مورد اعتماد پایبند باشید:

از نسخه های رسمی برنامه ها استفاده کنید و از نصب هر گونه پوسته یا نسخه غیر رسمی خودداری کنید.



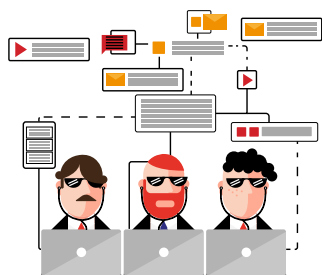
به طور منظم به روز رسانی کنید:

همیشه برنامه های شبکه های اجتماعی خود را به روز نگه دارید تا در برابر آسیب پذیری های امنیتی محافظت کنید.



احتیاط در شبکه های اجتماعی خارجی:

پلتفرم های خارجی فاقد استانداردهای حفاظت از حریم خصوصی در جاسوسی دولتی می باشند.



گزارش فعالیت مشکوک:

بلافاصله حساب های جعلی، کلاهبرداری یا رفتار غیرعادی را به تیم پشتیبانی شبکه اجتماعی گزارش دهید.

نتیجه گیری:

در حالی که شبکه های اجتماعی برای ارتباطات و کسب و کارهای اینترنتی در ایران ضروری هستند، اما با خطرات امنیتی همراه هستند. با پیروی از دستورالعمل های فناوری اطلاعات و هوشیاری، می توانید از اطلاعات شخصی خود و شرکت در برابر تهدیدات احتمالی محافظت کنید.