راهکارهایی برای امنیت در شبکه‌های اجتماعی

محدود کردن اطلاعاتی که پست می‌کنید

اطلاعاتی که ممکن است برایتان دردسرساز شود، مانند آدرس یا برنامه‌های روزانه‌تان از جمله اطلاعات محرمانه شما هستند. اگر دوستان و اطرافیانتان اطلاعاتی از شما پست کردند، مطمئن شوید در حدی باشد که آگاهی غریبه‌ها از آن مشکل‌ساز نشود. همچنین به اطلاعاتی که خود از اطرافیانتان پست می‌کنید هم توجه کنید. به یاد داشته باشید که اینترنت، مکانی عمومی است؛ فقط اطلاعاتی را پست کنید که با دیده یا خوانده شدن آن مشکلی نداشته باشید. هر آنچه پست کنید، به محض اینکه به فضای آنلاین رفت، دیگر برگشت‌پذیر نیست؛ حتی اگر حذفش کنید، ممکن است ورژن ذخیره‌شده یا cache آن در سیستم‌های دیگر باقی مانده باشد.

تنظیمات خود را بازبینی کنید

از تنظیمات محرمانگی سایت‌ها نهایت بهره را ببرید. تنظیمات پیش‌فرض برخی تارنماها، امکان دیده‌شدن مطالب شما را به دیگران می‌دهد؛ اما شما می‌توانید با تغییر کوچکی آن را محدود به افراد خاصی بکنید. با این همه، باز هم ممکن است اطلاعات شما دیده شود؛ پس حواستان باشد چه اطلاعاتی را آشکار می‌سازید. ممکن است سایت‌ها به‌طور منظم آپشن‌های خود را تغییر دهد، پس تنظیمات خود را مرتبا بازبینی کنید تا از درست‌بودن آن‌ها اطمینان حاصل کنید.

مراقب اپلیکیشن‌های شخص ثالث باشید

این اپلیکیشن‌ها برنامه و سرگرمی فراهم می‌کنند؛ اما مراقب باشید چه نرم‌افزاری را فعال می‌کنید. از برنامه‌های مشکوک بپرهیزید و تنظیمات خود را برای محدودکردن مقدار اطلاعاتی که برنامه‌ها به آن دسترسی دارند، تغییر دهید.

این روزها حضور در شبکه‌های اجتماعی بسیار زیاد شده است. افراد مختلف با سن، تحصیلات، جنسیت و شغل‌های مختلف در این شبکه‌ها عضو هستند و کاربران روزنامه میلیون‌ها بار به انتشار مطالب مختلف اقدام می‌کنند. اما زندگی در چنین فضایی آدابی دارد که باید به آن‌ها توجه ویژه‌ای کرد تا کمتر آسیب ببینیم و از مشکلات جدی جلوگیری شود. در ادامه به برخی اقدامات ساده در راستای افزایش امنیت در حوزه شبکه‌های مجازی اجتماعی را به شما گوشزد می‌کنیم، امیدواریم که مورد استفاده شما قرار بگیرد؛ اما با این حال فراموش نکنید که با همه این موارد، باز هم شما در معرض خطر هستید!

مراقب بیگانه‌ها باشید

اینترنت، تغییر هویت را برای افراد ساده ساخته است. تعداد افرادی را که می‌توانند با شما ارتباط داشته باشند، در شبکه‌های اجتماعی محدود کنید. اگر با کسی که نمی‌شناسید ارتباط دارید، مراقب میزان اطلاعاتی که آشکار می‌سازید و قرارهایی که می‌گذارید باشید.

مرورگر خود را به‌روز نگه دارید

نرم‌افزار خود را به‌روز نگاه دارید تا هکرها نتوانند از ضعف‌های امنیتی به شما ضربه بزنند. بسیاری از سیستم‌عامل‌ها امکان به‌روزرسانی خودکار را دارند، بهتر است آن را فعال کنید.

شکاک باشید

هر آنچه آنلاین می‌خوانید و می‌بینید، باور نکنید. افراد می‌توانند اطلاعات نادرست یا جهت‌داری را در موضوعات مختلف مانند هویتشان پست کنند؛ هرچند ممکن است عامدانه نبوده و اغراق یا حتی شوخی باشد. به هر روی مراقب باشید و به منبع و موثق‌بودن اطلاعات خود مطمئن شوید، پیش از آنکه دست به هر کاری بزنید.

خط‌مشی محرمانگی سایت‌ها را چک کنید

برخی سایت‌ها اطلاعات و ایمیل کاربران را با سایت‌های دیگر به‌اشتراک می‌گذارند که به افزایش اسپم می‌انجامد. همچنین ارجاعات خود را بازبینی کنید تا از فرستاده‌شدن اسپم به دوستان خود جلوگیری کنید. برخی سایت‌ها ارسال ایمیل به دوستان شما را تا زمانی که به آن‌ها بپیوندند، ادامه می‌دهند.

پسوردهای قوی برگزینید

برای اکانت‌های خود پسوردهایی برگزینید که نتوان به‌راحتی آن‌ها را حدس زد. اگر رمزهای عبور شما ساده باشد، دیگران به‌راحتی می‌توانند به اکانتتان دسترسی پیدا کنند و خود را به‌جای شما جا بزنند.