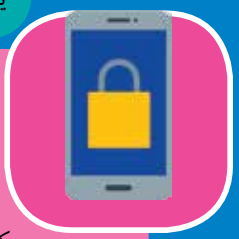
سعید چگینی

امنیت در شبکه‌های اجتماعی

محافظت از اطلاعات حساب‌های کاربری

از رمز عبور پیچیده استفاده کنید. رمز عبور طولانی (حداقل ۸ کاراکتر)، ترکیبی از حرف‌های کوچک و بزرگ انگلیسی و عددها و نمادها می‌تواند از حساب کاربری شما حفاظت کند. اگر احتمال می‌دهید که رمز عبور را فراموش کنید، از نرم‌افزارهای نگهداری اطلاعات کاربری همچون «کی‌پس»[1] (KeePass) استفاده کنید.

به یاد داشته باشید، رمز عبور به تنهایی ضامن امنیت حساب کاربری نیست. برخی اپلیکیشن‌ها و سرویس‌ها از موارد مکمل رمز عبور استفاده می‌کنند که با عنوان تأیید هویت دو مرحله‌ای یا «Two-Step Verification» شناخته می‌شود. یعنی کد تأیید توسط پیامک به تلفن همراه مالک حساب کاربری فرستاده می‌شود یا توسط اپلیکیشن‌هایی موسوم به «آتنتیکیتور»[2]، هر چند ثانیه یک رمز یک‌بارمصرف تولید می‌شود.



امنیت اطلاعات شخصی

اطلاعات شخصی و موارد مربوط به زندگی خصوصی‌تان را در فضای مجازی و اینستاگرام رها نکنید. اینکه شمارهٔ ملی، تاریخ دقیق تولد شما، نشانی و شمارهٔ تلفن منزل شما چیست، به کسی کمکی نمی‌کند، ولی طعمهٔ خوبی برای شیادان و کلاه‌برداران است. یا اینکه اگر می‌خواهید به سفر بروید یا الان با خانواده در سفر هستید، ممکن است به سارقان برای ورود بدون مزاحمت به منزل شما کمک کند.

دقت داشته باشید، هر آنچه را که در فضای مجازی به اشتراک می‌گذارید، دیگر نمی‌توانید پس بگیرید. در شبکه‌های اجتماعی می‌توانید با استفاده از تنظیمات حریم خصوصی، این موضوع را که چه کسانی اطلاعات شخصی شما را ببینند، مدیریت کنید.

امنیت اطلاعات مالی

میزان موجودی حساب بانکی شما یک مورد کاملاً خصوصی است و نام کاربری و رمز عبور حساب‌های بانکی شما بسیاربسیار خصوصی‌تر. اولین اشتباه موجب ضرر هنگفتی خواهد شد. هیچ نهادی حتی خود بانک نیز نمی‌تواند و حق ندارد که از شما اطلاعات حساب بانکی و نام کاربری و رمز عبور را تلفنی سؤال کند. اگر برندهٔ قرعه‌کشی شده‌باشید نیز هیچ کس از شما رمز حساب یا حضور در کنار عابربانک را درخواست نمی‌کند. پس حسابی مراقب اندوخته‌های مالی خود باشید.

استفاده از نرم افزارها و اپلیکیشن‌های «اصلی»[3]

همواره نرم‌افزارها و اپلیکیشن‌های مورد استفادهٔ خود را از وب‌سایت‌ها و منابع معتبر خرید یا دریافت کنید. سارقان اینترنتی به راحتی می‌توانند با تغییر متن برنامه‌ها، بدون اطلاع شما از همهٔ اطلاعات تلفن همراه شما جاسوسی کنند و همهٔ تصویرها و متن‌های شما را به سرقت ببرند.

در مواردی، برخی اپلیکیشن‌ها را برای افزایش تعداد «دنبال‌کننده‌ها»[4] و مدیریت حساب شبکه‌های اجتماعی نصب می‌کنیم و با وارد کردن اطلاعات حساب کاربری یا اجازهٔ دسترسی به موارد مختلف، راه را برای سرقت اطلاعات و حتی در برخی موارد، مسدود کردن دسترسی مالک حساب کاربری و اخاذی و افشای اطلاعات شخصی هموار می‌سازیم.

ضمناً اپلیکیشن‌های خود را همیشه به‌روزرسانی کنید. در این به روزرسانی‌ها، مشکلات و ایرادهای امنیتی از طرف شرکت سازنده برطرف می‌شوند.

اسکن کنید و امنیت شبکه‌های اجتماعی را بهتر بشناسید.

استفاده از نرم‌افزارهای امنیتی

یکی از راهکارهای مدیریت و مقابله با نفوذ، استفاده از اپلیکیشن‌ها و نرم‌افزارهای امنیتی است. این اپلیکیشن‌ها با مدیریت و رصد دائم دستگاه شما، نرم‌افزارهای مخرب، کرم‌های اینترنتی و درگاه‌های نفوذ را شناسایی می‌کنند و با مسدود و حذف کردن آن‌ها، ریسک از دست دادن اطلاعات را بسیار کاهش می‌دهند.

اعتماد

اعتماد یکی از مهم‌ترین عوامل در ارتباط انسان‌هاست. در زندگی روزمره نیز اعتماد زمینه‌ساز دادوستد و ارتباطات اجتماعی می‌شود. در فضای مجازی نیز این گونه است. آشنایی و به دنبال آن اعتماد، موجب آغاز یک رابطهٔ دوستانه و تعمیق آن بین افراد در طول زمان می‌شود.

حال فرض کنید که یکی از دوستانتان در یکی از شبکه‌های اجتماعی از شما درخواست مبلغی قرض می‌کند که باید به حساب دیگری واریز شود. این یکی از ترفندهای کلاهبرداران اینترنتی است. شیادان با استفاده از نام و هویت جعلی شما و با راه‌اندازی صفحه‌های مشابه یا دسترسی غیرمجاز به صفحهٔ کاربری شما، از دوستانتان درخواست مبلغی پول یا اطلاعات و حتی تصویرهای شخصی می‌کند.

حتی اگر دیدید لینکی در پیامی از سوی دوست شما فرستاده شده است، هنگام کلیک کردن روی آن بااحتیاط باشید. به این علت که ممکن است حساب کاربری دوست شما آلوده شده باشد و تلفن همراه یا رایانهٔ شما را نیز آلوده کند.

فضای شبکه‌های اجتماعی مملو از کاربرانی است که با هویت‌های جعلی و برای مقاصد خاص مثل کلاهبرداری و سایر اقدامات غیرقانونی و مجرمانه می‌کوشند با کاربران ارتباط بگیرند. از این‌رو از پذیرفتن افرادی که با طرح مطالب و تصویرهای اغواکننده سعی در ارتباط‌گیری و افزودن شما به فهرست دوستان یا علاقه‌مندان صفحهٔ خود را دارند، اجتناب کنید.

این روزها هر یک از ما در یک یا چند شبکهٔ اجتماعی حضور داریم و روزانه زمان نه‌چندان کمی را در اپلیکیشن‌های شبکه‌های اجتماعی می‌گذرانیم.

جامعهٔ مجازی نیز همانند جامعهٔ واقعی دارای اصولی است که برای حفظ امنیت و ارتباط گسترده باید به آن پایبند باشیم. مثلاً همان‌گونه که ما افراد غریبه را به خانه و یا جمع‌های خانوادگی راه نمی‌دهیم، در فضای مجازی و شبکه‌های اجتماعی نیز با افراد غریبه باید با احتیاط‌تر برخورد کنیم.

برای حفظ امنیت در شبکه‌های اجتماعی باید چه کنیم؟

پی‌نوشت‌ها

۱. WWW.KEEPASS.INFO

۲. AUTHENTICATOR

۳. ORIGINAL

۴. FOLLOWERS