فناوری و رسانه

یادداشت

ایزوله فیلم دیدن و جدایی نسل‌ها

ونوس بهنود
دبیر تحریریه
vbehnood@gmail.com

در مطالعات میدانی که صورت گرفته است، ایرانی‌ها یکی از مهم‌ترین سرگرمی‌های خود را فیلم و سینما تعریف کرده‌اند اما روند تماشای فیلم در طول دهه‌های اخیر به حدی تغییر کرده که گویای دردی عمیق در گسست نسل‌ها است.

زمانی که تلویزیون‌های سیاه و سفید برای اولین بار به خانه‌ها راه یافت، به‌دلیل اینکه هنوز قدرت خرید این جعبه جادویی برای همه فراهم نشده بود، خانواده‌ها در خانه یکدیگر جمع می‌شدند و فیلم تماشا می‌کردند. فیلم‌ها نه صحنه منشوری داشت و نه محتوایی که افراد را به سمت خشونت، بدکلامی و بدرفتاری هدایت کند. به همین دلیل تجربه فیلم دیدن دسته‌جمعی یکی از خاطراتی است که اگر از متولدان دهه‌های ۲۰ و ۳۰ بپرسید به شیرینی از آن یاد می‌کنند.

در آن مقطع زمانی سینماها نیز به تعداد محدود و در شهرهای محدود دایر بود و شهروندان اندکی به سینما دسترسی داشتند. حتی فیلم دیدن در سینما نیز با روح جمعی تماشاگران همراه می‌شد و بعد از تماشای فیلم، حس خوشایند برابری به همه انتقال می‌داد. بعدها وقتی تعداد تلویزیون‌ها در خانه‌ها بیشتر شد و این جعبه‌های جادویی، رنگی نیز شدند، تعداد برنامه‌هایی که پخش می‌شد افزایش یافت و هر گروه سنی می‌توانست برنامه‌های خود را تماشا کند. روزها برای کارتون و سرگرمی ویژه کودکان و شب‌ها برای فیلم ویژه بزرگسالان. اما همچنان تلویزیون در بخشی عمومی از خانه جانمایی می‌شد و تماشای انحصاری وجود نداشت. گوشی هوشمند با ورود خود به زندگی آدم‌ها ایزوله‌ای را رقم زد که موجب شد حتی نسل‌ها از هم جدا شده و روح جمعی لذت از محتوای رسانه در هم شکند. روز به روز محتواها اختصاصی و اختصاصی‌تر شد تا جایی که نوجوان گوشی به دست می‌توانست در اتاق خود بنشیند و فیلم مورد علاقه‌اش را تماشا کند، بدون اینکه آن را به والدین خود توصیه کند یا اینکه در تماشای آن بخواهد اشتراکی ایجاد کرده باشد.

ایزوله‌سازی رسانه‌ها موجب شده تا فرایندی که پژوهشگران از آن تحت عنوان هم‌تماشاگری (co-viewing) یاد می‌کنند درهم شکند و دیگر تماشای دسته جمعی یک برنامه به میزان قابل توجهی کاهش یابد. این پدیده را هم می‌توان از منظری مثبت و مفید مشاهده کرد و هم از منظری منفی. در شرایطی که هم‌تماشاگری نداریم، کنترل محتواها برای خانواده درحد غیرممکن شده است. از طرفی آدم‌ها حریم خصوصی بیشتری دارند و می‌توانند مطابق سلیقه خود به تماشای فیلم و برنامه بنشینند. رسانه‌ها شهروندان را هر روز در دیوارهای شیشه‌ای خود محصورتر و محصورتر می‌کنند و با تعریف محتوا متناسب با سلیقه کاربر، او را از تعاملات اجتماعی بویژه با خانواده جدا می‌کنند. تصور کنید زن و شوهری که هر یک در گوشی همراه خود محتوایی را تماشا می‌کند و حاضر نیست به همسر خود آن را توصیه کند تا مبادا برای دیدن فلان بخش آن محتوا لازم به پاسخگویی باشد. حباب شیشه‌ای رسانه هر چند نامرئی است اما اکسیژن زیست جمعی را کاهش داده است و روزی فرا می‌رسد که ما از شدت تنهایی احساس خفگی خواهیم کرد و آیا برای مواجهه و ممانعت از آن روز فکری اندیشیده‌ایم؟

گوشی هوشمند با ورود خود به زندگی آدم‌ها ایزوله‌ای را رقم زد که موجب شد حتی نسل‌ها از هم جدا شده و روح جمعی لذت از محتوای رسانه در هم شکند

اخیراً هک اطلاعات و دسترسی به داده‌های محرمانه به حدی با شیطنت سارقان اینترنتی افزایش داشته که انتخاب گذرواژه مناسب یکی از ضرورت‌ها جهت محافظت از داده‌های شخصی است، اما چگونه می‌توان به گذرواژه مناسب و غیر قابل هک رسید؟ سایت Nord pass اعلام کرده رمزهای آسان بهترین دستاویز برای هکرها است و به‌عنوان مثال رمزی مانند ۱۲۳۴۵۶ می‌تواند به سادگی هک شود. مروری داشته باشیم به ویژگی‌های پسوردهای ضعیف و قوی و نحوه انتخاب گذرواژه مناسب.

همه گذرواژه غیرقابل انتخاب کنید

مراحل انتخاب یک پسورد قوی

۱- پسوردهای قوی طولانی هستند

اولین چیزی که باید موقع ساخت رمز عبور به خاطر داشته باشید این است که پسوردتان طولانی باشد. یک رمز عبور قوی باید حداقل ۲۰ حرف داشته باشد. اگر گذرواژه شما ۸ حرف یا کمتر باشد، در ۵۸ ثانیه شکسته می‌شود.

۲- پسوردهای قوی نمادهای خاصی دارند

یک رمز ورود قوی باید شامل نمادها، اعداد، حروف کوچک و بزرگ باشد. درج علائم و اعداد خاص حدس رمز ورود شما را دشوارتر می‌کند چون شما با استفاده از این نمادها ترکیبات احتمالی بیشتری ایجاد می‌کنید. اگر پسوردتان شامل نمادها و کاراکترهای خاص باشد، احتمال اینکه قربانی حمله هکرها شوید کمتر می‌شود. هکرها موقع حمله و تلاش برای نفوذ به اطلاعات، ترکیب‌های مختلف حروف را امتحان می‌کنند تا رمز ورود شما را حدس بزنند و به حساب کاربری‌تان نفوذ کنند.

۳- رمزهای عبور قوی شامل اطلاعات واضح و مشخص نمی‌شوند

خیلی‌ها موقع انتخاب پسورد از اعداد یا حروفی که برایشان آشنا است استفاده می‌کنند؛ مثلاً تاریخ تولد، شماره شناسنامه، کد پستی یا آدرس، اما یادتان باشد چنین پسوردهایی امن نیستند و هکرها به راحتی می‌توانند آنها را شناسایی کنند. شما نباید از اطلاعات شناسایی شخصی به‌عنوان بخشی از رمز عبور خود استفاده کنید، اما این مسأله به این معنا نیست که حتماً باید اعداد، حروف یا عبارت‌های تصادفی را به کار ببرید. پسوردهای تصادفی شاید قوی باشند اما به خاطر سپردنشان مشکل است.

ویژگی‌های گذرواژه‌های ضعیف:

- گذرواژه‌ای که تنها از حروف کوچک تشکیل شده باشد.
- استفاده از نام خودتان، نام حیوان خانگی، تاریخ تولد یا اسامی رایج.
- گذرواژه‌ای که بین یک تا ۶ کاراکتر داشته باشد.
- استفاده از کلمات رایج مثل Apple، Book، Picture و...
- استفاده از پسوردهای تکراری.
- استفاده از ترکیب دکمه‌های کیبورد.

ویژگی‌های گذرواژه‌های معمولی:

- ترکیبی از حروف و اعداد.
- تشکیل شده از حداقل ۸ کاراکتر.
- استفاده از حروف کوچک و بزرگ.
- استفاده از اعداد و سَمبل‌ها.
- استفاده نکردن از کلمات دیکشنری.

ویژگی‌های گذرواژه‌های قوی:

- ترکیبی از حروف کوچک و بزرگ، اعداد و سَمبل‌ها.
- دارای بیش از ۸ کاراکتر.
- استفاده از عبارات من‌درآوردی.
- استفاده نکردن از کلمات کامل.
- آپدیت کردن رمزعبور در بازه‌های زمانی مشخص.

۴- پسوردهای قوی در خاطر می‌مانند و در آنها از کلمات اختصاری و کدها استفاده می‌شود

یک رمز عبور قوی باید در ذهن بماند وگرنه اصلاً خوب نیست. علاوه بر این، رمز عبورتان نباید طوری باشد که برای به خاطر سپردنش مجبور باشید آن را روی کاغذ بنویسید یا جایی در کامپیوترتان ذخیره کنید. حالا سؤال اینجا است که چطور می‌شود یک پسورد قوی که به راحتی در ذهن بماند انتخاب کرد؟ برای این کار سعی کنید از کدها و کلمات اختصاری مربوط به چیزهای خاصی که به راحتی در ذهنتان می‌مانند استفاده کنید. به این ترتیب رمز عبورتان برای همه بجز خودتان به صورت مجموعه‌ای تصادفی از حروف، اعداد و نمادها به نظر می‌رسد.

۵- رمز عبورهای قوی، احراز هویت چند مرحله‌ای دارند

متأسفانه چیزی به اسم رمزی که به هیچ وجه نتوان آن را هک کرد وجود ندارد؛ بنابراین احراز هویت دو مرحله‌ای بهترین راه برای ایمن نگه داشتن رمز عبورتان است. با این حال احراز هویت چند عاملی (MFA) نباید جایگزین ساختن یک پسورد قوی شود، بلکه باید به‌عنوان راهی برای محافظت از رمز عبورتان از آن استفاده کرد. MFA و تنظیمش رایگان است و یک لایه امنیتی اضافی به حساب کاربری شما اضافه می‌کند.

۶- پسوردهای قوی در پسورد منیجر ذخیره می‌شوند

پسورد منیجرها (Password manager) آسان، رایگان و ضروری هستند که می‌توانند همه رمزهای عبورتان را یکجا نگه دارند. با این کار دیگر نیازی به یادآوری ۵۰ گذرواژه مختلف نخواهید داشت، اما برای ورود به سیستم پسورد منیجرتان هم به یک رمز عبور قوی، امن و به‌یادماندنی نیاز دارید. خوبی استفاده از پسورد منیجرها این است که فقط باید یک پسورد را به خاطر بسپارید، اما در عین حال همین مسأله لزوم انتخاب یک رمز عبور قوی را مهم‌تر می‌کند.