



رسانه

ضمیمه نوجوان

شماره ۳۲ | آبان ۱۳۹۹

نوجوانان

سواد رسانه‌ای

وحشت از جنس مومو!

علیرضا عالی بیگی
مدال آور المپیاد سواد
رسانه‌ای / دوره چهارم



بعد از چند سالی که فکر می‌کردیم بالاخره از دست مومو و اون چهره خوفناک و هیپنوتیزم‌کننده‌اش راحت شدیم، دوباره نگرانی مادر و پدرها و ترس و وحشت بچه‌ها گریبان مارو گرفته!

شاید پرسید مومو اصلا چی هست؟!

و چطوری باعث این هرج و مرج‌ها شده؟!

مومو یه عروسک با چهره و طراحی ترسناک و کاملا حساب شده است که عکسش روی پروفایل برخی شماره‌های ناشناس واتس‌اپ دیده می‌شه!

خب حالا بذارید بهتون بگم منظور از طراحی حساب شده چی هست. بسیاری از کارشناسان می‌گن، موی بلند سیاه، بینی کوچک، عریضی لب‌ها و سیاهی دورچشم‌ها از حقه بیرون زده این مومو خان، نگاه‌ها را به سمت چشم‌های ترسناک او سوق میدن و باعث ایجاد نوعی حس کنترل‌گری ناخودآگاه مومو روی ما می‌شن!

براساس نوع بازی، ماموریت‌ها و نوع ترساندن بازیکنان که از طریق گفتن نشونه‌هایی از افراد و موقعیت مکانی آنها و... از تماس اون‌ها با ارگان‌های مربوط مثل پلیس جلوگیری می‌کنن، می‌تونیم بگیم، چالش مومو جایگزینی برای ننگ آبی و به گفته آمارها و حرف و حدیث‌ها، اولین قربانیش از آرژانتین بوده!

اما توی ایران به نظر میاد، حس شوخ‌طبعی نوجوونای ما جلوی فکرهای عاقلانه‌شون رو گرفته! براساس تحقیقات پلیس فتا، بیشتر شماره‌های ناشناسی که عکس پروفایل آنها چهره دلربای مومو است، مربوط به جوونا و نوجوون‌های خودمونه که قصد شوخی و دست انداختن دوستان خودشون رو دارن. حتی اپلیکیشن‌هایی هست که اگر نشد مومو رو ببینید، میتونید نصبش کنید و تماس تصویری فیک (جعلی) با مومو بگیرید!

این عمل‌های به ظاهر خنده‌دار و دروغین افراد در فضای مجازی، نتایج و خسارات جبران‌ناپذیری برای والدین و کودکان دردیای واقعی به همراه داره!

پس بیایید با همدیگه قبل از کارهای به‌ظاهر خنده‌دارمون به نتایج گریه‌دار اونا فکر کنیم و با عمل‌های پیشگیرانه نذاریم این عروسک مضحک و دلربا بلای جان ما و زندگی ما بشه!

ترس از هیچ!

چند سال پیش بود که خبری مبنی بر تازه‌ترین روش اعدام در جهان (در محافل خبری منتشر

شد؛ به‌گونه‌ای که فرد محکوم روی تختی خوابانده می‌شد و چشم‌هایش را می‌بستند سپس به بهانه تخلیه خون از بدنش لوله‌هایی به بدن او وصل می‌کردند و از آن آب ولرم رد می‌کردند؛ پس از مدتی فرد بدون خارج شدن حتی یک قطره خون از بدنش می‌میرد!

این نقل امروز ما در چالش‌های مجازی است؛ چالش‌هایی که با ایجاد رعب و وحشت کار خود را شروع می‌کنند و با شایعات سریع‌جا خود را در بین مردم باز می‌کنند و نهایتاً مجالی می‌شوند برای اخاذی عده‌ای سوءاستفاده‌گر...

حتما اسم چالش نهنگ آبی برایتان آشناست؛ چالشی که چند وقتی در صدر اخبار و شایعات بود و به دغدغه اصلی نوجوانان



حواس جمع!

عرفان قاسمی
مدال آور المپیاد
سواد رسانه‌ای



با بازگشت مجدد مومو، دوباره زمزمه‌های حفظ حریم شخصی و امنیت در فضای مجازی سر زبان‌ها افتاد؛ در این بخش چند نکته ساده و مهم درباره حفظ امنیت در فضای مجازی را با هم مرور خواهیم کرد.

۱. از تأیید دو مرحله‌ای استفاده کنید!

این قابلیت به معنای ایجاد دو لایه امنیتی برای دسترسی به حساب کاربری شماست و با فعال‌سازی آن، یک سد حفاظتی دیگر برای ورود به حساب کاربری شما ایجاد خواهد شد. خوشبختانه امروزه تمام سرویس‌های آنلاین شناخته شده مانند: گوگل، فیس‌بوک، اینستاگرام، تلگرام، واتس‌اپ و... این قابلیت را در دسترس کاربران قرار داده‌اند. برای فعال‌سازی تأیید دو مرحله‌ای، بخش تنظیمات امنیتی نرم‌افزار را جست‌وجو کنید!

۲. در انتخاب گذرواژه دقت کنید!

هکرها و بدافزارها معمولاً فاهرستی از گذرواژه‌های رایج و پرستفاده را در اختیار دارند و هنگام ورود به یک حساب کاربری از آنها استفاده می‌کنند، به همین علت به هیچ عنوان از کلمات رایج و قابل حدس به عنوان گذرواژه استفاده نکنید. بهتر است گذرواژه شما ترکیبی از حروف، اعداد و علائم نگارشی باشد. اگر به خاطر سپردن گذرواژه‌ها برایتان امری دشوار است، می‌توانید از نرم‌افزارهای مدیریت پسورد مانند: Bitwarden و lastpass

و خانواده‌های نگران‌شان تبدیل شده بود! این چالش با شعار «پاک کردن زمین از افراد به درد نخور» شروع به کار کرد و نهایتاً در دادرسی متهم ثابت شد که وی صرفاً برای شهرت این ادعا را کرده و اصلاً چالشی وجود نداشته است!

حالا هم چالشی جدید از شرق زمین سرو کله‌اش پیدا شده با نام MOMO؛ تصویر عروسکی عجیب و در عین حال ساده که همان‌طور که من با بزرگ نوشتن کلمات برجسته‌اش کردم با ویژگی‌های بصری خاص در ناخودآگاه ذهن مخاطب تأثیر می‌گذارد و او را مجذوب «ترس از هیچ» می‌کند!

این نوع چالش‌ها با استفاده از دسترسی‌هایی که ما خودمان به شبکه‌های اجتماعی داده‌ایم مثل: دسترسی به میکروفن، دوربین، موقعیت مکانی، مخاطبان و... اطلاعات ما را با ایجاد رعب و وحشت به خودمان برمی‌گرداند و در قبال آن درخواست عملی خطرناک یا پرداخت رشوه برای پایان بازی دارند!

جالب‌تر این که احتمال مواجهه شما با MOMO‌های تقلبی و افراد شاید بیشتر از برخورد شما با خود این چالش است که اصلاً ماهیت اصلی‌اش هم زیر سوال است!

در این ایام کرونایی که فضای مجازی تبدیل به مدرسه شده و برخورد ما با رسانه‌ها از هر زمانی بیشتر شده یادمان باشد در رسانه این دروغ و بزرگ‌نمایی‌ها هستند که اغلب اوقات روی ما تأثیر می‌گذارند؛ در مواجهه با پیام از طرف MOMO بدون دیدن پیام، آن شماره و اکانت آن را مسدود کنیم و مراقب باشیم با تلقین ذهنی اعدام نشویم!

می‌کنید، مدل تلفن شما و... بینجامد، که این اطلاعات برای یک هکر مفید خواهد بود!

۵. علایق تان را فریاد نزنید!

فضای مجازی بستر امنی برای به اشتراک‌گذاری علایق شخصی‌تان نیست. این کار در نگاه اول منطقی به نظر می‌رسد که علایق و شادی‌هایتان را با افرادی که شما را دنبال می‌کنند تقسیم کنید اما اگر فرد نامحرمی به این جزئیات دست پیدا کند، می‌تواند با تحلیل و استفاده از آنها، ویژگی‌های روان‌شناختی و نقاط ضعف و قوت شما را استخراج کرده و در مواقع مختلف از جمله در روابط فردی از آنها استفاده کند!

۶. گول نخورید!

بسیاری از افراد با استفاده از آگاهی کم دیگران نسبت به فناوری، اقدام به سوءاستفاده از آنها می‌کنند. برای جلوگیری از چنین اتفاق‌هایی باید سطح دانش خود نسبت به فناوری را بالا ببریم؛ برای این‌کار بهتر است پیش از نصب هر نرم‌افزار، سیاست‌های حفظ حریم خصوصی و شرایط استفاده از خدمات آن را مطالعه کنیم تا با دسترسی‌ها و ضوابط امنیتی آن آشنا شویم!

استفاده کنید. این نرم‌افزارها همچنین قابلیت انتخاب گذرواژه تصادفی و امن رانیز در اختیار شما قرار می‌دهند. برای کاهش احتمال لورفتن گذرواژه‌تان بهتر است هر چندماه یک‌بار گذرواژه‌هایتان را تغییر دهید.

۳. مراقب دسترسی‌ها باشید!

هر نرم‌افزاری به واسطه امکاناتی که در اختیار شما قرار می‌دهد نیازمند دسترسی به بخش‌های مختلف سیستم شما خواهد بود. دسترسی به موقعیت جغرافیایی، حافظه داخلی، دوربین، میکروفن و مخاطبان تنها بخشی از این مجوزها هستند. بدافزارها با دسترسی پیدا کردن به این بخش‌ها، به جاسوسی و افشای اطلاعات شما می‌پردازند.

با رفتن به بخش app permissions در تنظیمات تلفن هوشمندتان می‌توانید این مجوزها را لغو یا دسترسی‌های هر نرم‌افزار را محدود کنید.

۴. مخاطبان باهوش را دست‌کم نگیرید!

احتمالاً بارها شاهد انتشار عکس‌های سلفی، دسته‌جمعی و اسکرین‌شات‌های خود یا دیگران بوده‌اید. انتشار چنین تصاویری شاید در گام اول کم‌خطر به نظر برسد اما یک مخاطب زرنگ می‌تواند با در کنار هم قرار دادن تصاویری که منتشر می‌کنید به بخشی از اطلاعات شخصی شما پی ببرد. عکس‌هایی که از پنجره اتاقتان، محله‌تان و... می‌گذارید می‌تواند به لورفتن محل سکونت شما منجر شود. انتشار تصاویری که از صفحه تلفن‌تان گرفته‌اید هم می‌تواند به کشف نرم‌افزارهایی که استفاده

