

# جدال شبکه های اجتماعی با اخبار جعلی «کرونا»

میترا جلیلی خبرنگار

شیوع ویروس «کرونا» در چین و انتشار آن در سایر نقاط جهان نگرانی‌هایی را ایجاد کرده و البته انتشار سریع اخبار در شبکه‌های اجتماعی مختلف، دامنه مشکلات را گسترش داده است چراکه از همان لحظه آغازین اعلام خبرها درباره ویروس کرونا، اخبار جعلی و اطلاعات غلط درباره شیوع، درمان این بیماری و... در فضای مجازی منتشر شد. با توجه به سرعت بالای این انتشار، کمپانی‌های بزرگ فناوری و مالکان این پلتفرم‌ها برای مقابله با گسترش این اطلاعات غلط و اخبار جعلی و حذف آنها، دست به کار شدند.

■ **ابزار حقیقت‌یاب «فیس بوک»**

نام فیس بوک، توئیتر، تیک تاک و... در میان کمپانی‌هایی دیده می‌شود که تلاش می‌کنند تا راهکارهایی برای غربالگری انبوه اطلاعات موجود و ایجاد لینک‌هایی برای دستیابی کاربران به اطلاعات دقیق ارائه دهند. تعداد پست‌های حاوی اطلاعات غلط درباره شیوع این ویروس و همچنین راه‌های درمانی آن بسیار افزایش داشته و شبیه صعودی دارد. اما این شبکه‌های اجتماعی و غول‌های فناوری جهان چه راهکاری را مورد استفاده قرار داده‌اند تا در دام اخبار جعلی نیفتند و اصولاً چه تلاش‌هایی برای اطلاع‌رسانی درباره این بیماری داشته‌اند؟

یکی از شبکه‌های اجتماعی که در این زمینه گام‌های بلندی برداشته، فیس‌بوک است. این کمپانی در یک پست وبلاگی اعلام کرد دامنه انتشار اخبار غلط درباره ویروس کرونا را تا حد امکان کوچک خواهد کرد و برای این کار نیز حذف ادعاهای غلط یا سخنانی که از آنها پو می‌تونه برای ترساندن مردم و ایجاد رعب و وحشت به مشام می‌رسد را در دستور کار خود قرار داده است. فیس بوک در این پست وبلاگی ادامه داده است: پلتفرم ما از ابزاری

حقیقت یاب با نام fact-checkers استفاده می‌کند تا بتواند با مروری بر اخبار منتشر شده روی فیس بوک، نمونه‌های غیرواقعی و ادعاهای واهی را حذف کند. این کمپانی همچنین گفته است افراد حقیقی که پیش از این اخبار جعلی را منتشر کرده‌اند یا اینکه تلاش‌هایی برای به اشتراک‌گذاری اخبار غیرواقعی داشته‌اند را بیشتر زیر ذره بین دارد.

این شبکه اجتماعی بیش از همه بر ادعاهای درمانی برای مبتلایان به ویروس کرونا و ارائه نسخه‌های غلط درمانی آن تمرکز دارد. به‌عنوان مثال یک کاربر فیلپینی در فیس‌بوک راه درمانی برای مقابله با ویروس کرونا پیشنهاد داد و نوشت برای در امان ماندن از این ویروس اجازه ندهید گلوئ شما خشک بماند و همچنین از غذاهای پرادویه دوری کنید چرا که ویروس کرونا در این غذاها نهفته است. این پست بیش از ۱۶ هزار بار توسط کاربران به اشتراک گذاشته شد و بیشتر از ۴۰۰ کامنت دریافت کرد که در نهایت فیس‌بوک بلافاصله پس از اطلاع از این موضوع، این پست را از پلتفرم خود حذف کرد. اینستاگرام نیز که در مالکیت فیس‌بوک قرار دارد هشنگ‌هایی خاص با موضوع کرونا را مسدود کرد که البته اطلاعات غلط را رواج می‌دادند. واتس اپ، دیگر شبکه پیام رسان زیرمجموعه فیس‌بوک نیز به این کمپین فیس‌بوک پیوسته است و اجازه انتشار اخبار جعلی و دیتای نادرست را نمی‌دهد. این شبکه اجتماعی در گذشته هم مشکلات زیادی برای مقابله با انتشار اخبار جعلی داشت و به برخی کشورها همچون هندوستان درست مانند یک بمب ساعتی عمل می‌کرد چراکه در مواردی، انتشار اخبار غلط روی این پلتفرم به نزاع‌های گسترده و قتل منجر شد. سال گذشته این پلتفرم اعلام کرد که در راستای مقابله با انتشار اخبار جعلی، از ارسال انبوه پیام‌ها در این شبکه پیام رسان در برخی کشورها جلوگیری می‌کند.

به‌عنوان مثال در هندوستان کاربران نمی‌توانند از طریق واتس اپ یک پیام مشخص را به بیش از ۵ نفر یا ۵ گروه ارسال کنند. این پیام رسان همچنین پیام‌هایی که به دفعات فوروارد می‌شوند را تک می‌کند تا شناسایی شوند و در صورت قرار گرفتن در دسته اخبار جعلی، بتوان آنها را راحت‌تر شناسایی و حذف کرد.

■ **۱۵ میلیون توئیت درباره کرونا**

توئیتر نیز یکی دیگر از پیام رسان‌های محبوب جهان است که احتمال انتشار اخبار جعلی روی آن وجود دارد. توئیتر اعلام کرده است که از زمان اعلام شیوع ویروس کرونا تاکنون بیش از ۱۵ میلیون توئیت درباره این ویروس انجام شده است و با توجه به اهمیت موضوع، این پلتفرم امکانی را فراهم کرده که کاربران به محض جست‌وجو درباره کرونا و ویروس، به کانال‌های رسمی مربوط به سازمان جهانی بهداشت یا مراکز برای کنترل بیماری ارجاع داده شوند و اطلاعات درست و دقیق را به دست بیاورند. درواقع کاربران توئیتر به محض جست‌وجوی واژه کرونا ویروس با عبارت «واقعیت‌ها را بدانید» مواجه می‌شوند و با کلیک روی آن، عملاً به اطلاعات سازمان‌های رسمی و بهداشتی متصل می‌شوند. البته توئیتر اعلام کرده با اینکه تلاش‌های زیادی برای انتشار اخبار جعلی و حاوی اطلاعات غلط درباره این بیماری روی این پلتفرم دیده نمی‌شود اما ما همچنان هوشیار و گوش به زنگ هستیم تا از این تحرکات جلوگیری کنیم. ازسوی دیگر دانشمندان و پزشکان در توئیتر نیز از هشنگ‌های استفاده کرده‌اند تا آخرین اطلاعات درباره این ویروس، منبع بیماری، نشانه‌های بیماری و... را به اطلاع کاربران جهان برسانند.

■ **تیک تاک، اولین شبکه سلامت**

تیک تاک، این شبکه اجتماعی اشتراک‌گذاری ویدئو هم یک لینک به وب سایت سازمان جهانی بهداشت را فعال کرده و همچنین امکانی را در

اختیار کاربران قرار داده تا در صورت مواجهه با اطلاعات غلط درباره کرونا همچون راه‌های درمانی عجیب و غریب یا محتوایی که می‌تواند برای دیگر کاربران مضر باشد، بتوانند آن را گزارش دهند. اگر هم کاربران به دنبال اطلاعات بیشتری از این ویروس باشند می‌توانند با کلیک بر هشتگ کرونا ویروس (coronavirus) به اطلاعاتی گسترده دست پیدا کنند. البته این پلتفرم که در مالکیت شرکت چینی ByteDance قرار دارد، پیش از شیوع کرونا هدف انتقاداتی گسترده بود چراکه به پزشکان و پرستاران اجازه می‌داد در قالب پست‌های ویدئویی مشاوره‌های دارویی ارائه دهند اما حالا بسیاری معتقدند با تغییر استراتژی این پلتفرم، مشکلات پیشین آن نیز حل شود. تیک تاک البته با آور شده است که دستورالعمل این پلتفرم به گونه‌ای است که از انتشار محتوای مضر به طور کلی منع‌ت می‌کند.

■ **حذف محتوای دروغ در «یوتیوب»**

یوتیوب که در مالکیت گوگل قرار دارد نیز تاکنون در زمینه مقابله با انتشار ویدئوهای جعلی و حاوی صحنه‌های

خوشونت بار و همچنین محتوای سرشار از نفرت، تلاش بسیاری داشته و به عبارت دیگر چندان اجازه نمی‌دهد که کاربران قوانین و دستورالعمل‌های این پلتفرم را مورد حمله قرار دهند. این پلتفرم در زمینه ویروس کرونا نیز همین روند را ادامه داده و ویدئوها با محتوای غلط یا دروغ را به محض شناسایی، بسرعت حذف می‌کند.

■ **منابع معتبر در «رِدیت»**

یکی دیگر از شبکه‌های اجتماعی، ردیت (Reddit) است که به تازه واردان این پلتفرم هشدار می‌دهد مراقب محتوایی که درباره کرونا و...به اشتراک می‌گذارند، باشند درغیر این صورت اکانت آنها تعلیق می‌شود. این پلتفرم بر پایه گروه‌های بحث و تبادل نظر ساخته شده و کاربران می‌توانند به کامنت‌ها و پست‌هایی که سایر کاربران می‌گذارند، رای بدهند. این ساختار تا حدی به این پلتفرم کمک می‌کند تا از اطلاعات غلط در امان بماند اما با این حال این شبکه اجتماعی در صفحه نخست ردیت، یک اعلامیه قرار داده است که کاربران را با رشته‌ای از سؤال و جواب‌ها درباره کرونا ویروس، راهنمایی



نیوویز کینیاد

می‌کند. گفتنی است که منابعی معتبر در اختیار کاربران نگران از شیوع این ویروس قرار گرفته است.

■ **«اسنپ چت»، یک پلتفرم امن**

اسنپ چت نیز یکی دیگر از شبکه‌های اجتماعی است که برای مقابله با اطلاعات غلط درباره کرونا، اعلام آمادگی کرده است. این پلتفرم اعلام کرده که ساختار این شبکه اجتماعی تا حد زیادی از انتشار اخبار جعلی و غلط معانعت می‌کند چراکه پست‌های اسنپ چت بعد از ۲۴ ساعت ناپدید می‌شوند و همچنین کاربران اجازه ندارند پست‌ها را به دفعات زیاد به اشتراک بگذارند. همچنین این شبکه اجتماعی نیوز فید یا خبرخوان عمومی ندارد که هرکسی بتواند روی آن پست بگذارد البته این بدان معنا نیست که کاربران به‌صورت انفرادی نمی‌توانند در اسنپ چت اخبار جعلی به اشتراک بگذارند بلکه به این معناست که این پست‌ها تنها توسط تعداد کمی از افراد دیده می‌شود. به هر حال این شبکه اجتماعی نیز اعلام کرده که اجازه انتشار اخبار جعلی درباره کرونا را نخواهد داد.

وزیر ارتباطات و فناوری اطلاعات:

رؤیایا آینده را می سازند



وزیر ارتباطات و فناوری اطلاعات در جمع نخبگان المپیادی کشور از آنان خواست که هدف داشته باشند و برای رسیدن به رؤیایهای خود تلاش کنند.

خبر

به گزارش «ایران»، محمدجواد آذری جهرمی در گردهمایی فناوران فضایی و در جمع نخبگان و المپادی‌های دانش آموز و دانشگاهی بعد از شنیدن سخنان و دغدغه‌های نخبگان با اشاره به اینکه باید برای آینده خود هدفی ترسیم کنیم، به نخبگان دانش آموز و دانشجو توصیه کرد: برای خود هدف داشته باشید و به آن هدف افتخار کنید و برای رسیدن به آن تلاش کنید.

وی با اشاره به اینکه بسیاری از واقعیت‌های امروز تحقق رؤیایهای گذشتگان است، افزود: دیگران رؤیایهای ما را ساختند و ما نیز باید تلاش کنیم رؤیایهای دیگران را بسازیم و اگر این کار را انجام ندهیم آیندگان تصور خوبی نسبت به ما نخواهند داشت.

آذری جهرمی با اشاره به اینکه در مسیر رسیدن به آرزوها شکست نیز وجود دارد، گفت: بسیاری از افراد نسبت به اعلام خبر پرتاب ماهواره به دلیل شکست احتمالی انتقاد داشتند در صورتی که باید حقایق را به مردم بگوییم چرا که مردم دروغ گفتن را نمی‌پذیرند نه سخن گفتن از حقایق یا حتی شکست‌ها.

وی با اشاره به ساخت ماهواره‌های مختلف بعد از پیام ۱، افزود: ما از شکست ماهواره پیام ۱ درس گرفتیم و تلاش کردیم تا به رؤیایهای خود برسیم و حتماً موفق می‌شویم.

وزیر ارتباطات با تأکید به اینکه رؤیایا آینده را می‌سازد، گفت: این عرصه میدان تلاش است و تلاش زمانی معنی می‌دهد که رؤیای خوبی داشته باشیم. وی با بیان اینکه سازندگان ماهواره پیام ۱ در حال ساخت پیام ۲ هستند، افزود: این ماهواره با تکنولوژی روز جهان ساخته می‌شود.

آذری جهرمی با بیان اینکه با این تلاش‌ها به آینده روشن می‌رسیم، تأکید کرد: تمام فعالان این حوزه رؤیای کوبیدن پرچم ایران در کره ماه را دارند.

وی در بخش دیگری از سخنان خود به رئیس سازمان فضایی کشور دستور داد امکان رصد پرتاب ماهواره ظفر برای نخبگان نجوم فراهم شده و اطلاعات دریافتی از ماهواره برای تحلیل و ارزیابی به آنان ارائه شود.

در عین حال وزیر ارتباطات با بیان اینکه اولین گام برای اعزام فضاورد ایرانی به فضا برداشته شد، گفت: برنامه ساخت ۵ کپسول فضایی حمل انسان آغاز شد. وی گفت: این اولین گام برای اعزام فضاورد ایرانی به فضا خواهد بود که قرار است طی ۳ سال ساخته شود.

آذری جهرمی با بیان اینکه ساخت کاوشگر تاکنون در مرحله تحقیقاتی بوده است، افزود: هم‌اکنون ساخت ۵ کاوشگر را برای روبات‌های تا مدار ۱۹۰۰ کیلومتری زمین و در وزن هزار و ۸۰۰ کیلو سفارش داده‌ایم که نمونه اولیه برای آمادگی اعزام انسان به مدار زمین خواهد بود.

وزیر ارتباطات گفت: این پروژه با همکاری‌های بین‌المللی انجام می‌شود و تأثیر زیادی در پیشرفت دانش فضایی ایران در خصوص کاوش‌های فضایی خواهد داشت.

وی گفت: ما آرزو و هدفگذاری‌مان این است که به حضور ایرانیان در ماورای جو و سایر مدارات آسمانی برسیم و طبیعتاً اولین فاز این هدفگذاری، قرار دادن انسان در مدار زمین است.

وزیر ارتباطات و فناوری اطلاعات گفت: تحقیقاتی از قبل آغاز شده است و پژوهش‌هایی انجام شده که ما را امروز به این نتیجه رسانده است که پس از ۹ مرحله آزمون از ارسال سلول تا میمون به مدار زمین و تست قرار دادن موجود زنده بر مدار، آمادگی لازم برای اعزام انسان وجود دارد.

وی در مورد طراحی لباس فضاوردی که عکسی از آن را در شبکه‌های اجتماعی منتشر کرد بود، افزود: پروژه ساخت لباس فضاورد در دست اقدام است و در این مرحله لباس خیلی اولویت اول ما نخواهد بود. طبیعتاً ما از لباس‌های دیگر استفاده می‌کنیم که البته کاربران فضای مجازی در مورد عکسی که منتشر شد شوخی‌های خوبی کردند که ما از آنها تشکر می‌کنیم اما هدف این بود که اعلام خبر خوش در مورد ساخت کپسول فضایی صورت گیرد.

جهرمی در مورد آموزش برای فضاوردان ایرانی گفت: ما قرار نیست که به فضا توریست بفرستیم بلکه دانشمند ایرانی به فضا ارسال می‌کنیم. آموزش، جزئی از برنامه‌های ما است و قصد داریم فراخوان اعلام کرده و از دانشمندان فضایی که علاقه‌مند اعزام به فضا هستند ثبت‌نام کنیم.

## توئیتر به دنبال قوانین سختگیرانه علیه ویدئوهای جعلی



توئیتر قوانین سختگیرانه جدیدی را برای مدیریت ویدئوهای دستکاری شده که با استفاده از ابزار رسانه‌ای جعل عمیق (دیپ فیک) تولید شده‌اند، وضع کرد.

آن سوی خبر

به گزارش ایرنا، براساس قوانین جدید توئیتر دیگر نمی‌توان آن دسته از ویدئوهای مبتنی بر جعل عمیق را که آسیب‌های احتمالی به‌همراه دارند، در پلتفرم این شبکه اجتماعی منتشر کرد. به‌علاوه این شرکت همچنین با برچسب زدن بر توئیت‌های حاوی مضامین مبتنی بران فناوری، به افراد کمک می‌کند تا محتوای حقیقی را از محتوای دستکاری شده تشخیص دهند.

براین اساس، توئیتر از تاریخ ۵ مارس (۱۵ اسفند) بر توئیت‌های حاوی «محتوای دستکاری شده یا ساختگی» نشان می‌گذارد، دامنه دیده شدن آنها را محدود می‌کند و به کاربرانی که قصد لایک یا بازنشر چنین مضامینی را دارند، هشدار می‌دهد.

دیپ فیک (Deepfake) یا جعل عمیق نوعی فناوری برپایه هوش مصنوعی است که در تولید یا تغییر محتوای ویدئویی استفاده می‌شود تا ویدئوی نهایی نمایانگر چیزی باشد که در واقع اصلاً اتفاق نیفتاده است.

این تغییرات جدید نتیجه تلاش‌های مبارزه با فناوری جعل عمیق است. توئیتر که اواخر سال گذشته وعده وضع چنین قوانینی را داده بود، دستورالعمل‌های جدید را براساس بازخورد کاربران تهیه و تدوین کرده است.

با توجه به نزدیک شدن زمان انتخابات ریاست جمهوری آمریکا، به احتمال زیاد توئیتر به دنبال آن است تا از سواهی‌های سیاسی متکی بر فناوری جعل عمیق و به راه افتادن کمپین‌های اطلاعات نادرست جلوگیری کند.

## چگونه با هک حساب بانکی مقابله کنیم



آرژانتین

سینا آروش عضو انجمن کامپیوتر ایران

از نوع دیگر

با توسعه جوامع و دیجیتالی شدن ارتباطات اجتماعی و تجاری، شیوه‌های کلاهبرداری و مانورهای متقلبانه نیز فرآیندی فرا توسعه را تجربه می‌کند به عبارتی افکار کلاهبردارانه همچنان جلوتر از آگاهی‌های عمومی بوده و دائماً کاربران اینترنتی را تهدید می‌کند.

حالی که ما در این مقاله سعی داریم توضیح دهیم چگونه هکرها و آگاه باشیم تا مورد حمله هکرها قرار نگیریم. یکی از عمومی‌ترین روش‌های سرقت از حساب‌های بانکی، طراحی صفحات جعلی یا فیشینگ است. به این صورت که شما با یک جست‌وجوی ساده در اینترنت تمایل به خرید کالایی از طریق فروشگاه‌های اینترنتی دارید اما هکرها شما را به سایت جعلی خودشان برای پرداخت وجه که مشابه صفحه اصلی درگاه پرداخت بانک است هدایت می‌کنند و شما با وارد کردن اطلاعات حساب بانکی از جمله شماره کارت، رمز دوم، cv۲ و تاریخ انقضای کارت، همه اطلاعات لازم را ناخواسته در اختیار این دسته از افراد قرار می‌دهید. بنابراین اولین پیش‌اگاهی این است که شما باید از سایت‌های معتبر اینترنتی خرید کنید. برای این کار شما باید صفحات جعلی را از سایت اصلی درگاه‌های بانکی تشخیص دهید به‌عبارتی تمامی درگاه‌های بانکی در کشور دارای آدرس shaparak.ir دارند و این آدرس‌ها هستند اما اگر سایت با آدرس‌های مشابهی همچون shaparak.ir یا shaparak.ir بیا بود شما باید این تفاوت را تشخیص دهید و راه را برای نفوذ هکرها ببینید. نکته بعدی دقت به URL سایت است. توجه داشته باشید که قبل از آدرس هر سایتی که برای خرید اقدام می‌کنید در نوار آدرس بار، پروتکل

https قید شده باشد و اگر http بود، از خرید صرف نظر کنید زیرا وجود همین s کوچک امنیت اطلاعات تبادل شده را تضمین می‌کند. سومین مورد اینکه در تمامی سایت‌های معتبر خرید اینترنتی، لوگوی نماد اعتماد الکترونیکی نشان داده شده است اگر این نماد در صفحه موجود نباشد از خرید و ارائه اطلاعات بانکی صرف‌نظر کنید. یکی دیگر از راه‌های نفوذ هکرها، تلفن‌های همراه هوشمند است. در این شیوه از کلاهبرداری، هکرها با قرار دادن یک نوع ویروس در قالب یکی از نرم‌افزارهای بانکی یا حتی غیر بانکی که توسط خودشان طراحی شده است، به نفوذ در اطلاعات شخصی طعمه‌هایی پرداختند. گفتنی است که این ویروس‌ها هنگام تراکنش فعال می‌شوند و اطلاعات حساب را در اختیار هکرها اولین پیش‌اگاهی این است که شما باید از سایت‌های معتبر اینترنتی خرید کنید. برای این کار شما باید صفحات جعلی را از سایت اصلی درگاه‌های بانکی تشخیص دهید به‌عبارتی تمامی درگاه‌های بانکی در کشور دارای آدرس shaparak.ir دارند و این آدرس‌ها هستند اما اگر سایت با آدرس‌های مشابهی همچون shaparak.ir یا shaparak.ir بیا بود شما باید این تفاوت را تشخیص دهید و راه را برای نفوذ هکرها ببینید. نکته بعدی دقت به URL سایت است. توجه داشته باشید که قبل از آدرس هر سایتی که برای خرید اقدام می‌کنید در نوار آدرس بار، پروتکل

مجوز دسترسی به اجزای غیر مرتبط از جمله پیامک‌ها، مخاطبان، دوربین‌های تلفن و... را که هیچ کدام به بازی مربوط نیست، فعال نکنید. سومین راه نفوذ هکرها راهی به نام key logger است، در این روش هکر یک نوع ویروس را وارد دستگاه‌تان می‌کند که هر چه را می‌نویسید و تایپ می‌کنید، کی‌برداری کرده، برای هکر می‌فرستد و از این طریق به اطلاعات حساب بانکی و دیگر فایل‌های خصوصی‌تان دسترسی کامل پیدا می‌کند. برای جلوگیری از ورود اینگونه ویروس به تلفن‌هایماتان ابتدا باید یک آنتی ویروس قوی نصب کنید و به مسائلی که پیش‌تر به آنها اشاره کردیم، توجه کنید. چهارمین راه نفوذ، شنود از طریق تلفن همراه است، به این صورت که شما در ارتباط با حساب بانکی‌تان به مشکل می‌خورید و به جای مراجعه حضوری، با اپراتورهای بانک‌تان تماس می‌گیرید، عموماً در اینگونه مکالمات کاربران اطلاعات حساب بانکی‌شان را در اختیار اپراتور قرار می‌دهند تا مشکل‌شان حل شود که در این بین هکرها اطلاعات کاربران را دریافت و عملیات نفوذ را شروع می‌کنند.

برای جلوگیری از نفوذ، کاربران نباید

اطلاعات مهم حساب‌شان را از طریق تلفن یا پیامک برای اشخاص بازگو یا ارسال کنند. گفتنی است که کارکنان بانک هرگز اطلاعات مهم را تلفنی از شما دریافت نمی‌کنند و ضروری مشکل شما