دریچه

سیدمحسن سجادی:

قیمت دلار بزودی به پله قبلی برمی‌گردد

یک استاد اقتصاد با بیان اینکه قیمت دلار به زودی به پله قبلی برمی‌گردد، گفت: یکی از عواملی که به ثبات بازار ارز کمک کرد، کاهش رشد نقدینگی و کاهش رشد پایه پولی است، اما باید دقت کرد که کاهش رشد نقدینگی در زمانی که اقتصاد در رکود به سر می‌برد ممکن است خطر ساز شود، بنابراین باید سیاست کاهش رشد نقدینگی را در حدی که به اقتصاد آسیب وارد نکند ادامه داد. سید محسن سجادی؛ عضو هیات علمی دانشگاه مفید در گفت‌وگو با ایسنا گفت: کشور ما جزو کشورهای در حال توسعه است و برای اینکه به توسعه یافتگی دست یابیم ضروری است تا نرخ ارز به ثبات برسد، به عبارت دیگر ثبات بازار ارز پیش شرط رشد اقتصادی است. وی اظهار داشت: در کشور ما ثبات بازار ارز تاثیر زیادی بر رشد اقتصاد دارد زیرا برای بسیاری از کالاهایی که برای کشور ارزبری دارد و می خواهیم آنها را تولید و صادر کنیم هم نیاز به ارز داریم. بنابراین ثبات بازار ارز یکی از دستاوردهای مهم و بزرگ محسوب می‌شود. سجادی عنوان کرد: در اسفند سال ۱۴۰۱ نرخ ارز در کانال ۵۹ هزار تومان قرار داشت و اکنون بعد از حدود ۱۸ ماه شاهد هستیم که نرخ ارز تا هفته گذشته در همان محدوده قرار داشت که بعد از تنش‌های سیاسی و امنیتی در لبنان و فلسطین کمی بالاتر رفت اما موقتی است. این موضوع نشان می‌دهد در ثبات بازار ارز موفق بوده‌ایم. البته پیش بینی می‌شود قیمت دوباره ه پله‌های قبلی برگردد.

این تحلیلگر اقتصادی تصریح کرد: ثبات نسبی بازار ارز در حالی محقق شده است که طی این مدت شاهد انواع التهاب‌های سیاسی و نظامی بودیم که شامل بمب‌گذاری کرمان، حمله اسرائیل به سفارت ایران، حمله موشکی ایران به خاک اسرائیل، جنگ غزه و اسرائیل، صدور قطعنامه ضدایرانی در شورای حکام آژانس بین المللی انرژی اتمی، شهادت آقای رئیسی و شهید هنیه است. وی خاطرنشان کرد: در آخرین مورد حمله وحشیانه اسرائیل به لبنان و شهادت آقای سید حسن نصرا... بود که بازار ارز را اندکی ملتهب کرد، اما این التهاب نسبت به دوره‌های گذشته کمتر بود. این استاد دانشگاه ابراز کرد: در ثبات بازار ارز دائمی بودن درآمدهای ارزی مهم است یعنی تا زمانی که صادرات نفتی و غیرنفتی روند عادی خود را طی کند در کنار یک مدیریت مناسب، ثبات بازار ارز تداوم خواهد داشت. سجادی تاکید کرد: یکی از نکات مهم در مدیریت بازار ارز این است که تعیین نرخ ارز دستوری نباشد، چراکه دستوری بودن نرخ ارز به رشد اقتصادی کمکی نخواهد کرد، اما باید بر منابع و مصارف ارزی نظارت مورد نیاز وجود داشته باشد. عضو هیات علمی دانشگاه مفید تصریح کرد: طبق آمارها صادرات نفت ایران نسبت به سه سال گذشته چندین برابر شده است، همچنین براساس اعلام گمرک، تراز تجاری کشور با احتساب نفت به مثبت ۱۷ میلیارد دلار رسیده است، بنابراین افزایش درآمدهای ارزی به ثبات بازار ارز کمک خواهد کرد. وی خاطرنشان کرد: بازار ارز باید از لحاظ بنیادی تقویت شود. منظور از بنیاد بازار ارز همان تولید و صادرات است؛ یعنی با افزایش تولید و صادرات رشد اقتصادی محقق خواهد شد و رشد اقتصادی خود موجب تقویت ارزش پول ملی می‌شود. سجادی در پایان تاکید کرد: یکی از عواملی که به ثبات بازار ارز کمک کرد، کاهش رشد نقدینگی و کاهش رشد پایه پولی است، اما باید دقت کرد که کاهش رشد نقدینگی در زمانی که اقتصاد در رکود به سر می‌برد ممکن است خطر ساز شود، بنابراین باید سیاست کاهش رشد نقدینگی را در حدی که به اقتصاد آسیب وارد نکند ادامه داد.

کوتاه

۲/۹ میلیارد دلار قطعات خودرو وارد شد

در نیمه نخست امسال ۲۹۲ هزار تن اجزا و قطعات خودرو به ارزش ۲.۹ میلیارد دلار وارد کشور شد که به لحاظ وزن و ارزش به ترتیب ۱۷ و ۱۸ درصد کاهش نشان می‌دهد. به گزارش مهر، بر اساس اعلام گمرک ایران، در نیمه اول سال جاری ۳۲۹ هزار تن اجزا و قطعات خودرو و موتورسیکلت به ارزش ۳.۱ میلیارد دلار وارد کشور شده است. این میزان اجزا و قطعات خودرو و موتورسیکلت وارداتی به لحاظ وزن ۱۷.۶ درصد و از حیث ارزش ۲۰ درصد کاهش نشان می‌دهد. همچنین در این مدت ۱۰ هزار و ۸۶۵ تن به ارزش ۳۱.۶ میلیون دلار اجزا و قطعات خودرو و موتورسیکلت صادر شده که از لحاظ وزن ۱۳ درصد کاهش و از حیث ارزش ۸ درصد افزایش داشته است. بر اساس این گزارش، از مجموع صادرات اجزا و قطعات (خودرو و موتورسیکلت) در ۶ ماهه امسال، ۹ هزار و ۲۳۵ تن به ارزش ۲۶.۸ میلیون دلار به صادرات اجزا و قطعات خودرو و یک هزار و ۶۳۰ تن به ارزش ۴.۸ میلیون دلار به صادرات اجزا و قطعات موتورسیکلت اختصاص داشت.

«آرمان ملی» از پیامدهای منفی استفاده از ابزارها و فناوری‌های دیجیتالی در حوزه امنیتی - نظامی گزارش می‌دهد

ترور فناوری با دستان قاتلان حرفه‌ای

آرمان ملی - صدیقه بهزادپور: تهدیدات ناشی از سوءاستفاده از فناوری‌های نوین یکی از مهم‌ترین چالش‌های امنیتی در دنیای امروز است، اما با وجود پیشرفت‌های چشمگیر در حوزه فناوری، خطرات بالقوه‌ای نیز به همراه آنها به وجود آمده‌اند. برای مقابله مؤثر با این تهدیدات، نیاز به هماهنگی‌های گسترده، تقویت زیرساخت‌های امنیتی، تدوین قوانین و مقررات بین‌المللی و افزایش آگاهی عمومی وجود دارد. استفاده صحیح و مسئولانه از فناوری‌های نوین می‌تواند به حفظ امنیت ملی و عمومی کمک کند و از تبدیل شدن این فناوری‌ها به ابزار تهدید جلوگیری کند. کارشناسان معتقدند: تدوین قوانین و گسترش دیپلماسی فناوری در این راستا می‌تواند با اِعمال مجازات‌ها برای کشورها و گروه‌هایی که از فناوری‌ها و ابزارهای دیجیتال در راستای نیل به اهداف خود، با کشتارهای فردی یا گروهی مانند آنچه در لبنان رخ داد، فضای توسعه و رشد دیجیتالی را ناامن می‌سازند، از حاشیه‌های احتمالی در این عرصه پیشاپیش جلوگیری کنند.

به گزارش «آرمان ملی»، محمدرضا زنوزی، کارشناس حوزه فناوری در این باره گفت: تهدیدات ناشی از استفاده از فناوری‌های نوین دیجیتال و ابزار الکترونیکی، به‌ویژه در زمینه امنیت ملی و عمومی، یکی از چالش‌های مهم دنیای امروز است. نمونه‌هایی از این تهدیدات را می‌توان در حوادث مختلف جهانی مشاهده کرد که در آن گروه‌ها یا رژیم‌های مختلف از فناوری‌های پیشرفته برای حملات سایبری، انفجارها، جاسوسی و سایر ویژگی‌ها استفاده کرده‌اند. فناوری خود به طور بالقوه به‌عنوان تهدید تلقی نمی‌شود، اما یکی از نمونه‌های بارز این تهدیدات، انفجار پیجرها در لبنان است. در این حادثه، از پیجرها به‌عنوان ابزار انفجاری استفاده می‌شود که به شکلی مشخص می‌شود برخی افراد را هدف قرار می‌دهند، در حالی که مردم عادی نیز در این بین آسیب دیدند. در نتیجه شاهد این بودیم که ابزارهای دیجیتالی که در ابتدا برای ارتباطات و احساس راحتی عمومی طراحی می‌شوند، می‌توانند در دستان گروه‌ها یا همان هایی که به دنبال مقاصد ویژه هستند، به سلاح‌های خطرناک تبدیل شوند. فناوری هایی مانند تلفن‌های همراه، پهپادها، ابزارهای جاسوسی و حتی شبکه‌های اجتماعی، همگی می‌توانند در خدمت تخریب و... قرار گیرند. با افزایش پیچیدگی این ابزارها و دسترسی آسان به آن‌ها، خطرات آن‌ها برای امنیت ملی و بین‌المللی نیز افزایش یافته است.

روش‌های سوءاستفاده از فناوری‌های نوین

او افزود: یکی از متداول‌ترین شیوه‌های استفاده نادرست از فناوری، برنامه سایبری است. این برنامه می‌تواند شامل هک کردن شبکه‌های دولتی، مالی و زیرساخت‌های حیاتی باشد. برخی از کشورها یا گروه‌ها از این نوع ابزار برای دستیابی به اطلاعات حساس یا ایجاد بی‌ثباتی در سایر موارد استفاده می‌کنند. از سوی دیگر با پیشرفت فناوری‌های دیجیتال، جاسوسی نیز افزایش یافته است، استفاده از تلفن‌های همراه، کامپیوترها و حتی دوربین‌های هوشمند برای جمع‌آوری اطلاعات حساس از افراد، سازمان‌ها و دولت‌ها، به یکی از تهدیدات بزرگ برای امنیت ملی تبدیل می‌شود. استفاده از پهپادها برای عملیات نظامی یا جاسوسی نیز در این سال‌ها بعدی گسترش یافته است، هرچند این فناوری‌ها که در ابتدا برای مصارف غیرنظامی و تجاری طراحی شده بود، اکنون به سلاحی تبدیل شده است که می‌توان آن را با دقت به هدف مورد نظر انجام داد. این امر در خصوص شبکه‌های اجتماعی نیز صادق است، این شبکه‌ها نیز گاهی به بستری برای انتشار ایدئولوژی‌های افراطی و حرکت به خشونت تبدیل می‌شوند. گروه‌های تروریستی از این پلتفرم‌ها برای جذب نیرو، جمع‌آوری کمک‌های مالی، و برنامه‌ریزی از برنامه‌های کاربردی می‌کنند، از مصادیق این امر می‌توان به تشکیل گروه‌های داعش و... اشاره کرد که طی سالیان اخیر انجام شد. زنوزی توضیح داد: تهدیدات پنهان این ابزارها، با وجود کاربردهای مثبت‌شان، پتانسیل تهدید امنیت عمومی را نیز دارند. فناوری و ابزارهای دیجیتالی می‌توانند زیرساخت‌های حیاتی مانند برق، آب، و حمل‌ونقل و... را مختل کنند. همچنین، امور، افراد و جاهای مرتبط با فناوری‌ها و احتمال انفجار باعث ایجاد نگرانی‌های شدید بین مردم و امنیت می‌شود. از این رو لازم است برای مقابله با این امر دولت‌ها با سرمایه‌گذاری بیشتر اقدام به تقویت زیرساخت‌های امنیت سایبری را مدنظر داشته باشند. دولت‌ها باید با ایجاد نهادهای نظارتی قوی‌تر و کارآمدتر، بر استفاده از فناوری‌های نوین نظارت بیشتری داشته باشند. این نهادها می‌توانند مسئولیت تنظیم و تصویب استانداردها و مقررات لازم برای استفاده ایمن از فناوری را برعهده بگیرند. علاوه بر این، تقویت همکاری این نهادها با بخش خصوصی برای شناسایی تهدیدات فناوری‌های جدید ضروری است. شرکت‌های بزرگ فناوری باید به‌طور مداوم با نهادهای دولتی در ارتباط باشند و فناوری‌های خود را برای جلوگیری از سوءاستفاده‌ها تقویت کنند.

ایجاد سیستم‌های هشداردهی سریع

او ادامه داد: ایجاد سیستم‌های هشداردهی سریع برای شناسایی حملات سایبری یا تهدیدات فناوری یکی دیگر از راهکارهای مهم است که در بسیاری از کشورها در حال حاضر استفاده می‌شود. این سیستم‌ها باید به‌گونه‌ای طراحی شوند که هرگونه فعالیت مشکوک در فضای مجازی یا در استفاده از فناوری‌های دیجیتال را شناسایی و به سرعت به مقامات امنیتی گزارش دهند. استفاده از فناوری‌های هوش مصنوعی برای شناسایی زودهنگام تهدیدات می‌تواند به کاهش خطرات کمک کند. علاوه بر این مسئولان و سازمان‌های امنیتی باید فراتر از اقدامات محافظتی صرف رفته و برنامه‌هایی برای دفاع فعال در برابر تهدیدات فناوری داشته باشند. دفاع فعال به این معناست که به‌جای تنها واکنش نشان دادن به حملات، به‌صورت پیش‌دستانه تهدیدات شناسایی و خنثی شوند. این امر نیازمند تربیت نیروهای متخصص در زمینه امنیت سایبری، جنگ الکترونیک، و مقابله با حملات فناوری است.

ضرورت رصد و مدیریت فناوری‌های در حال توسعه

این کارشناس اضافه کرد: فناوری‌هایی که در حال توسعه هستند، مانند اینترنت اشیا (IoT)) واقعیت مجازی (VR) و هوش مصنوعی (AI) می‌توانند تهدیدات جدیدی برای امنیت ملی و عمومی ایجاد کنند. به همین دلیل، دولت‌ها و سازمان‌های بین‌المللی باید به‌طور مداوم این فناوری‌ها را رصد کنند و برای پیش‌بینی و مدیریت خطرات آنها برنامه‌ریزی داشته باشند. تدوین مقررات برای این فناوری‌ها قبل از آنکه به‌طور گسترده در دسترس قرار گیرند، از اهمیت زیادی برخوردار است. علاوه بر این زیرساخت‌های حیاتی کشورها مانند سیستم‌های انرژی، آب، حمل‌ونقل و ارتباطات به‌شدت در معرض تهدیدات سایبری و فناوری‌های نوین قرار دارند. هرگونه اختلال در این زیرساخت‌ها می‌تواند به بحران‌های بزرگ اجتماعی و اقتصادی منجر شود. تقویت امنیت این زیرساخت‌ها از طریق فناوری‌های پیشرفته مانند شبکه‌های رمزنگاری، پایش لحظه‌ای، و استفاده از نرم‌افزارهای دفاعی مدرن از اولویت‌های اصلی هر دولت باید باشد.

شفاف‌سازی مسئولیت‌ها و توسعه دیپلماسی دیجیتال

او معتقد است: یکی از چالش‌های پیش روی مقابله با تهدیدات فناوری این است که اغلب مشخص نیست چه کسی مسئول سوءاستفاده از این ابزارهاست. برای مقابله مؤثر با این تهدیدات، دولت‌ها و سازمان‌های بین‌المللی باید سازوکارهایی برای شناسایی مسئولین حملات دیجیتال و فناوری‌های مخرب تدوین کنند. این شامل ایجاد پیمان‌های بین‌المللی برای جلوگیری از استفاده نادرست از فناوری‌ها و پاسخگو کردن افرادی است که از این ابزارها برای اهداف خصمانه استفاده می‌کنند. بر این اساس؛ یکی از راهکارهای نوین در مقابله با تهدیدات فناورانه، توسعه دیپلماسی دیجیتال است. دیپلماسی دیجیتال به همکاری‌های بین‌المللی در زمینه امنیت سایبری و فناوری‌های دیجیتال اشاره دارد. کشورها باید از طریق دیپلماسی دیجیتال با یکدیگر در زمینه مقابله با تهدیدات فناوری همکاری کنند و به یک توافق جهانی برای استفاده مسئولانه از فناوری‌های نوین برسند. همچنین، می‌توان از این طریق به جلوگیری از رقابت‌های مخرب و تسلیحاتی در حوزه فناوری پرداخت.

ظرفیت‌های مثبت پنهان فناوری‌ها در ارتقای امنیت

با وجود اینکه فناوری‌ها می‌توانند به تهدید تبدیل شوند، اما همین فناوری‌ها نیز می‌توانند به افزایش امنیت کمک کنند. استفاده از هوش مصنوعی، بلاکچین و دیگر فناوری‌های پیشرفته برای محافظت از اطلاعات حساس و ایجاد سیستم‌های دفاعی قوی‌تر می‌تواند به مقابله با تهدیدات فناوری کمک کند. همچنین، توسعه فناوری‌های تشخیص تهدید و نرم‌افزارهای امنیتی می‌تواند به کاهش احتمال سوءاستفاده از فناوری‌های نوین کمک کند. یکی از جنبه‌های مهم در مقابله با تهدیدات فناوری، ایجاد فرهنگ مسئولیت‌پذیری در میان کاربران است. افراد باید درک کنند که استفاده از فناوری‌های نوین مسئولیت‌هایی نیز به همراه دارد. دولت‌ها و سازمان‌ها باید تلاش کنند تا با برگزاری کمپین‌های آگاهی‌بخشی و آموزش‌های عمومی، کاربران را با خطرات احتمالی و روش‌های ایمن استفاده از فناوری آشنا کنند.

رئیس سازمان بورس تاکید کرد:

صیانت از حقوق سرمایه‌گذاران بورسی

رئیس سازمان بورس و اوراق بهادار با اشاره به اینکه ماموریت اصلی این سازمان تسهیل تشکیل سرمایه است، گفت: صیانت از حقوق سرمایه‌گذاران از وظایف این سازمان است. سرمایه وقتی تشکیل می‌شود که سرمایه‌گذار احساس کند مورد صیانت و حمایت است.

«حجت ا... صیدی» روز (چهارشنبه) در چهارمین کنفرانس بین‌المللی راهبری شرکتی اظهار داشت: به دنبال این هستیم تا جایگاه نظام راهبری شرکتی را در بازار سرمایه ارتقا دهیم.

وی افزود: در همین راستا نیاز است تا از ابزار مقررات حاکمیت شرکتی برای بهبود وضع شرکت‌های فعال در بورس بهره بگیریم. در مرحله نخست باید از تصمیمات آنی خودداری کرد ضمن اینکه در این مسیر باید شرکت‌ها ملزم به شفافیت و انتشار دقیق اطلاعات شوند. صیدی با بیان اینکه یکی از مهم‌ترین وظایف سازمان بورس و اوراق بهادار در همه دنیا، صیانت از منافع سهامداران است، گفت: چند سال است که در ایران نرخ تشکیل سرمایه منفی است، در حالی که قرار بود رتبه نخست منطقه باشیم. به ترتیب در منطقه عربستان، ترکیه و امارات بالاتر از ایران قرار دارند. رئیس سازمان بورس اوراق بهادار افزود: برای اینکه سال آینده جایگاه نخست داشته باشیم باید ۵۵ درصد رشد اقتصادی داشته باشیم که ممکن نیست، اما برای اینکه در سال ۱۴۱۰ همین رتبه چهارم را حفظ کنیم باید ۵.۶ درصد رشد اقتصادی داشته باشیم. برای دستیابی به این هدف باید سالیانه بین ۱۵۰ تا ۲۰۰ میلیارد دلار تشکیل سرمایه داشته باشیم. وی عنوان کرد: مقررات حاکمیت شرکتی قبلا تدوین شده و یکبار نیز بازنگری شده است و ما الان در حال ارزیابی و تغییراتی روی آن هستیم، اما مسأله مهم چگونگی اجرای آن است. این مقام مسئول با اشاره به اینکه نظام راهبری شرکتی باید جدی گرفته شود، گفت: آموزش اهمیت زیادی دارد. فرآیندها باید اصلاح و کمیته انتصابات باید جدی گرفته شود. صیدی خاطرنشان کرد: دستورالعمل نظام راهبری شرکتی در بورس تنظیم شده و یک بار هم بازنگری شده است، ممکن است ۱۵ درصد دیگر هم تغییر کند. این تغییرات مهم نیست، مهم اجرای این دستورالعمل است که روی آن تاکید داریم.

وی با اشاره به اینکه متوسط حاشیه سود شرکت‌ها از ۲۳ به زیر ۱۲ درصد رسیده است، گفت: باید از سرمایه افراد صیانت شود و از مدیران شایسته در صدر شرکت‌ها برای افزایش و سود دهی شرکت‌ها استفاده شود.

تلنگر

امنیت لینک‌های ارسالی را جدی بگیرید!

با توجه به افزایش استفاده از اینترنت و فضای مجازی، کاربران باید نسبت به این تهدیدات آگاه باشند و از کلیک بر روی لینک‌های ناشناس خودداری کنند، بنابراین آموزش و افزایش آگاهی عمومی در این زمینه می‌تواند به کاهش خطرات ناشی از لینک‌های آلوده کمک کند. یکی از مشکلات امنیتی دیجیتال که روزبه‌روز و با سرعت دامنه وسیع‌تری پیدا می‌کند، انتشار لینک‌های آلوده یکی از چالش‌های جدی درزمینه امنیت دیجیتال است که به‌سرعت در حال گسترش است. این لینک‌ها معمولاً به‌عنوان بخشی از حملات سایبری طراحی‌شده‌اند و می‌توانند از طریق ایمیل، شبکه‌های اجتماعی، پیام‌رسان‌ها و... به کاربران ارسال شوند. هدف اصلی این لینک‌ها، فریب کاربران و هدایت آنها به سایت‌های مخرب یا آلوده است. این سایت‌ها ممکن است حاوی بدافزارهایی باشند که به سیستم کاربر آسیب می‌زنند یا اطلاعات حساس او را سرقت می‌کنند. همچنین، برخی از این لینک‌ها به صفحات فیشینگ هدایت می‌کنند که در آن‌ها تلاش می‌شود تا اطلاعات شخصی، مانند رمز عبور یا شماره کارت اعتباری، از کاربران دزدیده شود. با توجه به افزایش استفاده از اینترنت و فضای مجازی، کاربران باید نسبت به این تهدیدات آگاه باشند و از کلیک بر روی لینک‌های ناشناس خودداری کنند بنابراین آموزش و افزایش آگاهی عمومی در این زمینه می‌تواند به کاهش خطرات ناشی از لینک‌های آلوده کمک کند. درنهایت، استفاده از نرم‌افزارهای امنیتی معتبر نیز می‌تواند به شناسایی و مسدود کردن این تهدیدات کمک کند. علی اصغر زارعی - مدرس دانشگاه و کارشناس ارشد مدیریت سیستم‌های اطلاعاتی، مهندسی فناوری و اطلاعات - در گفت‌وگو با ایسنا، با بیان اینکه بسیاری از لینک‌هایی که کاربران دریافت می‌کنند، ممکن است به‌ظاهر معمولی و استاندارد به نظر برسند، اظهار کرد: حتی لینک‌های کوتاه شده نیز می‌توانند حاوی محتوای مخرب باشند و تشخیص آلوده بودن آن‌ها از روی ظاهر غیرممکن است؛ این به این معناست که کاربران نباید به سادگی بر اساس شکل و ساختار لینک‌ها، امنیت آن‌ها را ارزیابی کنند. وی افزود: برخی از لینک‌ها ممکن است به وب‌سایت‌های فیشینگ یا حاوی بدافزار هدایت کنند؛ برای حفظ امنیت، باید احتیاط بیشتری به خرج داده و از کلیک کردن بر روی لینک‌های مشکوک خودداری کرد؛ بنابراین هرگز سعی نکنید امنیت سایت‌ها را از ظاهر لینک‌ها تشخیص دهید. عضو کمیسیون کسب و کارهای مجازی و اقتصاد دیجیتال نصر کشور گفت: زمانی که یک لینک را دریافت می‌کنید، مهم است که قبل از کلیک کردن بر روی آن، احتیاط کنید، این لینک می‌تواند از طریق ایمیل، پیامک، شبکه‌های اجتماعی و یا... ارسال شده باشد. با توجه به اینکه برخی لینک‌ها ممکن است حاوی محتوای مخرب باشند، بررسی امنیت آنها ضروری است.

زارعی همچنین تشریح کرد: برای این کار، می‌توانید از ابزارهای آنلاین برای تحلیل لینک استفاده کنید یا آدرس را به‌طور دستی بررسی کنید. علاوه بر موارد گفته شده به نشانه‌های مشکوک در متن لینک یا فرستنده توجه کنید. این اقدامات می‌تواند به شما کمک کند تا از مشکلات امنیتی جلوگیری کنید و اطلاعات شخصی‌تان را حفظ کنید.

برای بررسی امنیت لینک‌ها، یکی از بهترین روش‌ها استفاده از سرویس‌های آنلاین رایگان است. این ابزارها به شما کمک می‌کنند تا خطرات احتمالی لینک‌ها را شناسایی کنید. استفاده از این وب‌سایت‌ها بسیار ساده و کاربرپسند است و تنها کافی است که لینک موردنظر را در قسمت جست‌وجوی سایت قرار دهید. پس از واردکردن لینک، با فشردن دکمه Enter، فرآیند جست‌وجو آغاز می‌شود. این بررسی معمولاً در چند ثانیه انجام می‌شود و نتایج به شما نمایش داده می‌شود. اگر نتیجه بررسی مثبت بود، به این معناست که لینک امن است و می‌توانید با خیال راحت روی لینک کلیک کنید و از آن استفاده کنید.

لیست برخی سایت‌های معتبر برای بررسی امنیت لینک‌ها است.

- https://safeweb.norton.com
- https://scanurl.net
- https://www.phishtank.com
- https://transparencyreport.google.com/safe-browsing/search https://www.virustotal.com
- https://www.psafe.com/dfndr-lab و https://www.urlvoid.com

این سایت‌ها به عنوان ابزارهای امنیتی عمل می‌کنند که هدف اصلی آن‌ها محافظت از کاربران در برابر تهدیدات سایبری است. تروجان‌ها نرم‌افزارهایی هستند که به‌ظاهر بی‌ضرر به نظر می‌رسند، اما می‌توانند به سیستم کاربر آسیب برسانند یا اطلاعات حساس را سرقت کنند.

باج‌افزارها (Ransomware) نوعی بدافزار هستند که پس از ورود به سیستم، فایل‌ها را قفل کرده و برای بازگشایی آن‌ها درخواست پول می‌کنند. ویروس‌ها نیز برنامه‌هایی هستند که می‌توانند خود را تکثیر کرده و به سیستم‌های دیگر منتقل شوند. حملات فیشینگ به روش‌هایی اشاره دارد که هکرها سعی می‌کنند اطلاعات شخصی کاربران را از طریق لینک‌های آلوده به دست آورند. درنتیجه، این سایت‌ها با شناسایی و مسدود کردن لینک‌های خطرناک، از کاربران در برابر این تهدیدات محافظت می‌کنند.

بنابراین با توجه به موارد گفته شده توصیه می‌شود بر روی لینک‌های موجود در ایمیل‌ها یا پیام‌های فوری کلیک نشود حتی اگر کاربر فرستنده‌ی آن را می‌شناسد. بنابراین بهتر است کاربران دست‌کم، ماوس را روی لینک نگه دارند تا مشاهده کنند آیا مقصد آن درست است یا خیر.

همچنین اگر نشانی وب‌سایت با «https» شروع نمی‌شود، یا نماد قفل بسته را در کنار URL مشاهده نمی‌کنید، از وارد کردن اطلاعات حساس یا دانلود فایل‌های آن سایت خودداری کنید. از سوی دیگر اگر حساب‌های آنلاین دارید، باید عادت کنید که به طور مرتب رمزهای عبور خود را عوض کنید. حساب‌های شما ممکن است بدون اطلاع شما در معرض خطر قرار گرفته باشند.