کد خبر: ۲۰۹۷۳۳
پنج شنبه ۱۵ آبان ۱۳۹۹ ۱۱:۰۰

کارمندان دورکار حتما بخوانند

شیوع ویروس کرونا در سراسر دنیا با همه تلخی‌ها، تجربیات جدیدی به همراه داشت و نشان داد که انسانها در این کره خاکی همچون دانه‌های تسبیح به یکدیگر وصلند و مرگ یک نفر به معنای مرگ دیگری است، به همین دلیل بارها توصیه شده که همه باید نسبت به پروتکل‌های بهداشتی تمکین کرده تا از مرگ انسان‌های بیشتر جلوگیری کنیم.

به گزارش سایت خبری پرسون، ویروس کرونا در ابتدا در دسامبر ۲۰۱۹ در شهر ووهان چین با همه‌گیری در انسان شیوع پیدا کرد و پس از مدت کوتاهی تمام جهان را فرا گرفت. در ایران نیز از ۲۹ بهمن ۱۳۹۸ به دنبال فوت دو بیمار در اثر ابتلا به این ویروس، اکنون کرونا جان حدود ۳۷ هزار نفر را در کشور گرفته است.

این در حالی است که استانهای تهران، اصفهان، قم، آذربایجان شرقی، خراسان جنوبی، سمنان، قزوین، لرستان، اردبیل، خوزستان، کرمانشاه، کهگیلویه و بویراحمد، گیلان، بوشهر، زنجان، ایلام، خراسان رضوی، مازندران، چهارمحال و بختیاری، البرز، آذربایجان غربی، مرکزی، کرمان، خراسان شمالی، همدان، یزد و کردستان در وضعیت قرمز قرار دارند و استانهای هرمزگان، فارس، گلستان و سیستان و بلوچستان نیز در وضعیت نارنجی و زرد قرار دارند.

مسئولان ستاد ملی مقابله با کرونا با اجرای محدودیت‌های جدید در ۲۵ مرکز استان و ۴۶ شهرستان دیگر محدودیت های جدیدی اعمال کردند زیرا روند بیماری کرونا در کشور صعودی است و حتما باید رعایت پروتکل‌های بهداشتی و محدودیت‌ها جدی گرفته شود.

یکی از مصوبات ستاد ملی مقابله با کرونا اعمال محدودیت حضور فیزیکی و ۵۰ درصدی کارکنان دستگاه های دولتی و غیر دولتی است.

براین اساس کرونا، فرصتی برای استفاده از تجربه دورکاری به وجود آورده و باید از دورکاری به عنوان ابزاری جهت افزایش بهره‌وری و کاهش هزینه‌ها استفاده کرد آن هم در شرایط کنونی که با موج سوم و تکان دهنده کرونا روبرو هستیم.

دورکاری فرصت جدیدی پیش روی افراد قرار داد که چگونه می توان با ابزارهای نوین ارتباطی در سرکار خود حاضر بود بدون اینکه حضور فیزیکی داشت فارغ از آنکه توسعه ابزارهای الکترونیکی و ارتباط جمعی بسیاری از کسب و کارها را به سمت فضای مجازی کشاند، این روزها کارمندان بخش های خصوصی و دولتی و همچنین معلمان و دانش آموزان از تجربه جدیدی در سراسر دنیا بهره مند شدند اینکه در منزل بمانند و فعالیت های روزانه خود را انجام دهند.

با وجود این ویژگی مثبتی که کرونا به بشر هدیه کرده اما مسائل امنیتی در دنیای مجازی نیز بسیاری از کاربران را تهدید می کند. این روزها که اغلب کارمندان در منزل به کار خود اشتغال دارند و در فضای گسترده و پیچیده فضای مجازی حضور دارند، باید بدانند که شیادان فضای مجازی نیز همچون آن ها در این فضا در حال گشت و گذار هستند و دنبال طعمه های خود می گردند براین اساس افزایش دانش در استفاده از این ابزارهای نوین لازم و ضروری است.

باید بدانیم درست است که اینترنت انجام فعالیت‌های شغلی به‌صورت دورکاری را تا حد زیادی تسهیل کرده اما علاوه بر به خطر انداختن حریم خصوصی افراد می‌تواند امنیت شرکت‌های خصوصی و مشاغل را نیز در معرض خطر جدی قرار دهد.

بسیاری از کارشناسان آی تی و همچنین پلیس فتا به کارمندان توصیه می کنند تا چگونگی استفاده امن از فضای مجازی و اینترنت را آموزش ببینند تا در اثر بی اطلاعی مورد هک یا سرقت اطلاعات قرار نگیرند حتی این مساله شامل مسئولان در بخش های مختلف می شود چرا که به دلیل همه‌گیری ویروس کرونا و دورکاری اکثر افراد جامعه، شاهد افزایش بی سابقه برگزاری ویدئو کنفرانس‌ها نیز هستیم.

شبکه‌های وای فای ناامن یکی از مهم‌ترین نقاط آسیب‌پذیر در فعالیت آنلاین محسوب می‌شود، باوجود اینکه بسیاری از کارمندان از اینترنت خانگی خود در زمان اجرای طرح فاصله گذاری اجتماعی و عدم حضور در محل کار استفاده می‌کنند و امکان تأمین امنیت آن را دارند، اتصال به شبکه‌های وای فای عمومی امکان دسترسی غیرمجاز به اطلاعات مهم را برای اشخاص ثالث فراهم می‌کند از سوی دیگر این امر می‌تواند موجب به خطر افتادن امنیت مجازی کاربران شود؛ زیرا معمولا این تجهیزات و شبکه‌ها فاقد ابزارهای امنیتی مورد استفاده در شبکه‌های سازمانی و شرکتی مانند نرم‌افزارهای ضدویروس قدرتمند، فایروال‌های سفارشی و ابزارهای پشتیبان گیری آنلاین هستند.

مهم‌ترین نکات امنیتی که کارمندان باید در زمان دورکاری رعایت کنند شامل استفاده از گذرواژه‌های مناسب، به‌روزرسانی مستمر سیستم‌عامل، اجتناب از باز کردن سایت‌ها و ایمیل‌های مشکوک، اعتبارسنجی دولایه یا تائید دومرحله‌ای، تأمین امنیت و انتخاب گذرواژه قوی برای مودم‌های خانگی است.

روش‌های حفظ امنیت در استفاده از وای فای عمومی

یکی از ابزارهای کارمندان در زمان دورکاری استفاده از اینترنت است استفاده از آن نیز ملزم به استفاده از داده یا وای فای است.

کارشناسان پلیس فتا معتقد هستند که تهدیدات سایبری و روش‌های بهبود امنیت سیستم‌های رایانه ای به منظور حفظ امنیت افراد دورکار در دوران مقابله با شیوع ویروس کرونا بسیاری جدی است و باید برای استفاده از اینترنت برای اجرای امور کاری محوله خود از وای فای عمومی به علت عدم رعایت مؤلفه‌هایا امنیتی، ستفاده نکنند.

همچنین توصیه می شود برای هر حساب کاربری خود از کلمه عبور قوی شامل یک رشته طولانی از حروف بزرگ، کوچک، اعداد و کارکترهای ویژه استفاده شده و برای چند حساب کاربری از یک کلمه عبور مشترک استفاده نشود.

در صورت استفاده از مودم‌های ADSL، کلمه عبور پیش فرض آن را تغییر و از خاموش بودن قابلیت WPS دستگاه، اطمینان حاصل کنند. به صورت متناوب و در بازه زمانی لازم، پشتیبان‌گیری از داده‌ها را فراموش نکنند چرا که در صورت حمله سایبری یا هرگونه باج افزار آسیب کمتری به کار و اطلاعات آن ها وارد می شود.

کارشناسان پلیس فتا به افراد دورکار توصیه می کنند قبل از استفاده از دستگاه رایانه خود، یقین پیدا کنید که فایروال دستگاه فعال و آنتی‌ویروس قدرتمند و به‌روز شده نصب باشد.

همچنین مواظب ایمیل‌های مشکوک به کلاهبرداری و فیشینگ اطلاعات که برای آن ها ممکن است، ارسال شود، باشند و به هیچ عنوان لینک‌ها و ایمیل‌های مشکوک را باز نکنند.

چنانچه مجبور هستید در یک فضای عمومی کارکنید یا اگر با افرادی زندگی می‌کنید که نمی‌توانید اطلاعات کار را با آنها به اشتراک بگذارید، امنیت دستگاه رایانه مهم است و پیشنهاد می شود تا رمز ورود به دستگاه خود را فعال کنید.

برای اطمینان از امنیت بیشتر حساب‌های کاربری خود پس از تعیین رمز عبور ترکیبی قوی از مؤلفه احراز هویت دومرحله‌ای از جمله اسکن اثر انگشت یا تأییدیه پیامکی استفاده کرده و در صورت نداشتن اطلاعات تخصصی کافی در این زمینه از مشاوره کارشناسان معتمد کمک بگیرند.

چند توصیه به کارمندان برای امنیت فضای مجازی

- از اعتبارتان در شبکه‌های اجتماعی مراقبت کنید زیرا مواردی را که آنلاین پست کنید در اینترنت یا روی دستگاه بقیه کاربرها می‌ماند. قبل از اینکه عکس یا پستی را ارسال کنید، حتما قبل از آن مطمئن باشید که بعدا پشیمان نمی‌شوید. در نظر بگیرید که برخی درخواست‌های شغلی تنها به خاطر پست‌های متقاضیان در شبکه‌های اجتماعی رد شده‌اند.

- موقعیت‌های مختلف را شناسایی کنید و عکس‌العمل صحیحی داشته باشید، اگر شخصی مزاحم است یا پست و عکس خشونت‌آمیز نسبت به گروه خاصی منتشر کرده است، حتما آن را گزارش دهید و از دایره دوستان خود خارج کنید.

- نرم‌افزارهای روی دستگاه خود را به روز نگاه دارید زیرا مرورگر، سیستم عامل و تمام نرم‌افزارهایی که روی دستگاهتان است را به روز نگاه دارید. به روز بودن نرم‌افزارها جلوی تهدیدهای سایبری زیادی را می‌گیرد.

- تا جایی که امکان دارد حساب خود را شخصی نگاه دارید تا روی افرادی که ما را دنبال می‌کنند یا دوست‌مان هستند کنترل داشته باشیم. کنترل بدین معنی است که اجازه ندهید شخص غریبه پست‌ها و عکس‌های شما را ببیند.

- کلمه عبور پیچیده، تصادفی و طولانی انتخاب کنید و مطمئن شوید که کلمه عبورتان حداقل ۱۲ حرف را دارد که شامل حروف کوچک، بزرگ، اعداد و حروف خاص است. این کلمه عبور باید کاملا تصادفی باشد. برای این کار می‌توانید از نرم‌افزارهای مدیریت رمزعبور مانند LastPass استفاده کنید.

- هر حساب کاربری آنلاینی که دارید، باید رمز عبور منحصربفرد خودش را داشته باشد. یک رمزعبور را برای بیش از یک حساب کاربری استفاده نکنید.

- هرگز از دستگاه‌هایی که متعلق به شما نیستند، آنلاین خرید نکنید. همچنین از شبکه‌ای که به امنیت آن مطمئن نیستید نیز برای خرید آنلاین استفاده نکنید. در غیر اینصورت داده‌های شما توسط هکرهای خرابکار کپی می‌شود.

- مجرمان اینترنتی اغلب از پروفایل‌های جعلی برای شروع دوستی با هدف خود استفاده می‌کنند. هدف اکثر آن ها به دست آوردن اعتماد و سپس گرفتن اطلاعات از کاربران است اگر برایتان امکان‌پذیر است نرم‌افزار آنتی‌ویروس را از شرکت مطمئن خریداری کنید. مطمئن شوید که آنتی ویروسی که استفاده می‌کنید به روز و قابل اعتماد باشد.

- یکی از مهم‌ترین نکته‌های حفظ امنیت دیجیتال این است که در هر حسابی که می‌توانید از گزینه احراز هویت دو عامله استفاده کنید. کد دوم را می‌توانید از طریق SMS یا اپلیکیشن دریافت کنید. در نظر داشته باشید هر چقدر تعداد لایه‌های امنیتی بیشتر باشند، امنیت اطلاعات خود بیشتر حفظ می‌شود.

- فعالیت‌های آنلاین خود را ردیابی کنید، لیست تمام حساب‌های آنلاین خود را داشته باشید و به روز رسانی خودکار نرم‌افزارها را فعال کنید چرا که به

روز رسانی نرم‌افزارها و اپلیکشن‌ها از بیش از ۸۵ درصد حمله‌های سایبری افراد را حفظ می کند.

- سیستم عامل و تمام نرم‌افزارها و اپلیکیشن‌هایی که روی آن نصب کرده‌اید را به روز کنید. بیشتر نرم‌افزارها گزینه به روز رسانی خودکار را دارند، آن را فعال کنید.

- باج‌افزارها یکی دیگر از تهدیدهای بزرگ امنیت دیجیتال هستند. این نوع بدافزار یا سیستم عامل شما را قفل می‌کند که بدان دسترسی نداشته باشید یا اطلاعات‌تان را رمزنگاری می‌کند. مجرم اینترنتی در این نوع حمله از قربانی درخواست باج می‌کند تا اطلاعات و سیستم عاملش را به او برگرداند.

مجموعه توصیه های ارائه شده سبب می شود تا در بحران کرونا، بیشتر دچار آسیب نشویم و بدانیم که عده ای هستند که همیشه و در بدترین شرایط و بحران ها برای رسیدن به منافع خود سوء استفاده می کنند وبنابراین تنها سپر محافظت از خود در برابر آن ها، افزایش و آگاهی و به روز کردن اطلاعات خود در تمام عرصه ها است.

منبع: ایرنا