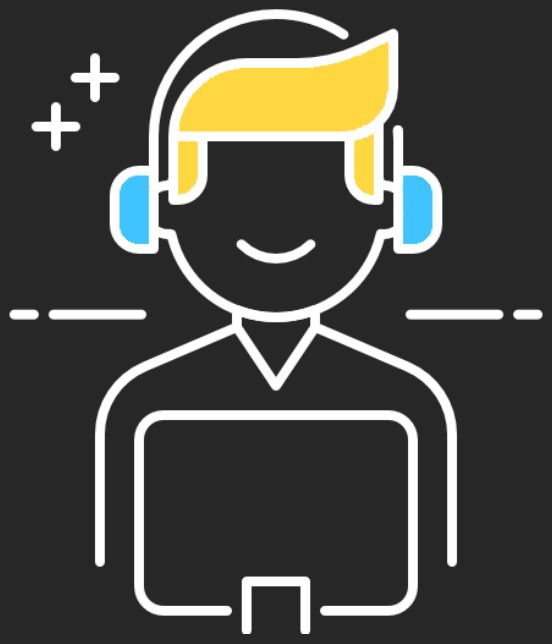

چک‌لیست اصول امنیتی دورکاری

Ravro

برای دورکارها و دورکارترها :

دو سال پیش هم شاید خیلی از ما دورکار بودیم و بقیه هم راجع به دورکاری شنیده بودیم. اما از یک سال پیش که کووید ۱۹ مهمان ناخوانده‌ی جهان شد، همه‌گیریش باعث شد که به ناچار در خیلی از جزئیات سبک زندگیمان تغییراتی بدهیم؛ اگر دورکار نبودیم، شدیم و اگر هم که دورکار بودیم، دورکارتر شدیم.

دورکاری هم مثل خیلی از چیزهای دیگر، هم مزایای خودش را دارد، هم معایبش، هم اصول و آداب مخصوصش. ما در این مطلب اصول امنیتی موردتاکید جهانی [1] و پیشنهادهای امنیتی خود را برای شما در چهار بخش خلاصه کرده‌ایم، نکاتی که در:

- در وب‌گردی‌های خود
- در حین کار با سیستم خود
- در سامانه‌های کاری خود
- در جلسات و هم‌کاری‌های خود
- و اگر مسئول آی‌تی یا امنیت هستید

بهتر است در نظر داشته باشید و رعایت کنید تا دورکاری امن‌تری را تجربه کنید.

به هرحال، هر جای دنیا هم که باشیم، چه در دنیای حقیقی و چه در دنیای مجازی، به امنیت نیاز داریم.

[1] Remote Working Cybersecurity Checklist , Cyber Management Alliance Ltd. (CM-Alliance)

در وب‌گردی‌های خود:

- **به آدرس لینک‌هایی که به دست شما می‌رسند، دقت کنید.**

گاهی افراد سودجو در صدد هستند با ایجاد دامنه‌هایی مشابه دامنه‌های اصلی و معتبر که تنها در کاراکترها و جزئیات محدودی تفاوت دارند، افراد را به ورود به صفحه‌ی قلابی تدارک‌دیده‌شده ترغیب و با استفاده از غفلت آن‌ها، اطلاعاتشان را از طریق فیلدهای ورودی دریافت کنند. این فرآیند فیشینگ نام دارد و فیشینگ ممکن است از طریق ایمیل یا حتی پیامک به سراغ شما بیاید.

- **نسبت به لینک یا سند مشکوک و نامطمئن درباره‌ی موضوعات جنجالی روز مانند ویروس کرونا حساسیت بیشتری داشته باشید و بر روی هر لینکی کلیک نکنید.**

موضوعات جنجالی روز، دام مناسبی برای ترغیب افراد به کلیک هستند. این لینک‌ها که اغلب به سایت‌های ناشناس باز می‌شوند، خطرناکند و امکان دانلود خودکار و اجرای بدافزارهای مختلف بر روی سیستم شما را فراهم می‌کنند. در موارد دیگری نیز، این لینک‌ها برای اجرای حمله‌ی فیشینگ طراحی شده‌اند. (توجه داشته باشید که حمله‌ی فیشینگ فقط مختص درگاه‌های بانکی نیست و صفحه‌ی ورود هر سامانه‌ای نیز می‌تواند دامی برای فیشینگ باشد.)

- **مراقب باشید که مورد سوءاستفاده‌ی سایت‌های غیراخلاقی قرار نگیرید.**

اغلب سایت‌های غیراخلاقی، با پیشنهاد دانلود فایل یا حتی دانلود خودکار یک فایل پس از ورود افراد، بدافزاری را به درون سیستم کاربر منتقل می‌کنند. این فایل‌ها که اجراکننده‌ی بدافزار هستند، می‌توانند آسیب زیادی به سیستم کاربر وارد کنند و یا محتواهای محرمانه‌ی موجود در سیستم را به سرقت ببرند.

- **در صورت دانلود نرم‌افزار یا ... از سایت‌ها، ابتدا فایل دانلودشده را برای کشف ویروس احتمالی اسکن کنید.**

به عنوان نمونه، نرم‌افزارهای موجود در سایت‌های دانلود به ویژه کرک‌های ارائه‌شده برای هرکدام از آن‌ها پتانسیل وجود بدافزار را در خود نیز دارند. در حالت ایده‌آل بهتر است از سیستم دیگری به غیر از سیستمی که برای فعالیت‌های کاری استفاده می‌کنید، برای کار با این سایت‌ها و سامانه‌ها استفاده کنید. برای اسکن بدافزارهای احتمالی در فایل دانلودشده، می‌توانید از سامانه‌های ویروس‌یابی نظیر https://virustotal.com استفاده کنید.

- **در صورت وقوع اشتباهی مانند ارسال ایمیل به آدرس اشتباه، کلیک بر روی یک لینک مخرب و مواردی از این دست، بهتر است هر چه سریع‌تر موضوع را با مسئول آی‌تی یا امنیت در میان بگذارید.**

- **بر روی تبلیغات و بنرهای سایت‌ها و برنامه‌هایی که مراجعه می‌کنید، کلیک نکنید.**

در بسیاری از سایت‌های فروشگاه‌های اینترنتی یا سایت‌های دانلود، صفحات پاپ‌آپ به طور خودکار باز می‌شوند، به شما بابت برنده‌شدن در یک قرعه‌کشی که حتی از آن خبر نداشته‌اید تبریک می‌گویند و از شما اطلاعاتی را طلب می‌کنند. در دام این سودجویان نیفتید و اگر لینکی را معرفی کردند به هیچ عنوان بر روی آن‌ها کلیک نکنید و فورا صفحه را ببندید.

هم‌چنین، بعضی بدافزارها در پوشش تبلیغات جذاب در سایت‌ها منتشر می‌شوند که البته با کمی هوش‌مندی قابل‌تشخیصند. مواردی نظیر تبلیغ فروشگاه‌های اینترنتی و محصولات مختلف لاغری و غیره از این قبیل‌اند که لینک آن‌ها مخرب است و فرد با مراجعه به آن لینک قربانی بدافزارهایی می‌شود که به صورت خودکار دانلود می‌شوند.

- **هنگام نصب برنامه‌ها و مراجعه به سایت‌ها، مجوز دسترسی‌هایی از شما گرفته می‌شود. لازم است هوشیار باشید و تنها اجازه دسترسی‌های معقول و مرتبط با عملکرد برنامه را بدهید.**

در صورتی که درخواست مجوز دسترسی به مواردی مانند میکروفن و دوربین از سمت برنامه و سایت غیرمنطقی می‌نمود، آن برنامه‌ها را نصب نکنید و به آن سایت‌ها نیز مراجعه نکنید.

- **از سیستم و صفحه‌نمایش آن به ویژه دسکتاپ در شبکه‌های اجتماعی، عکسی منتشر نکنید.**

انتشار تصویر از سیستم خود، اطلاعاتی راجع به نوع سیستم شما، برنامه‌های نصب شده بر روی آن، موقعیت مکانی و ... را در اختیار هکرها قرار می‌دهد که می‌توانند به آن‌ها در جمع‌آوری اطلاعات و مهندسی اجتماعی جهت نفوذ کمک کنند.

- **در پاسخ‌دادن به سوالات شخصی و مربوط به علایق خود در شبکه‌های اجتماعی احتیاط کنید و هوشیار باشید که پاسخ سوالاتی که برای بازیابی گذرواژه‌ی خود تعیین کرده‌اید را در فضای عمومی اعلام نکنید.**

پاسخ به سوالات شخصی می‌تواند به هکرها در فرآیند جمع‌آوری اطلاعات و مهندسی اجتماعی فرد هدف کمک کند. سوالاتی از قبیل "نام معلم شما چه بود؟"، "نام حیوان موردعلاقه‌ی شما چیست؟" و ... که در شبکه‌های اجتماعی پرسیده می‌شوند نیز گنجینه‌ی اطلاعات هکر راجع به مخاطب را کامل می‌کنند و شناخت فرد را برای هکر آسان‌تر و مسیر مهندسی اجتماعی را هموارتر می‌نمایند. علاوه بر این سوال‌ها، ممکن است از جمله سوالاتی باشند که در فرآیند بازیابی گذرواژه استفاده می‌شوند. همان‌طور که آگاهید یکی از راه‌هایی که سایت‌ها برای بازیابی گذرواژه پیش روی شما می‌گذارند پاسخ‌دادن به سوالاتی اغلب شخصی است که پیش‌تر پاسخ آن‌ها را از شما دریافت کرده‌اند. حال اگر شما ناآگاهانه پاسخ همان سوال‌ها را در شبکه‌های اجتماعی منتشر کرده باشید، کلید ورود به حساب کاربری خود را مستقیما در دسترس هکر قرار داده‌اید.

- **تنها کاری که لازم است برای امنیت بیشتر حساب کاربری اینستاگرام و تلگرام خود انجام دهید، فعال‌سازی تایید هویت دو مرحله‌ای است.**

هک حساب کاربری اینستاگرام یا تلگرام تقریبا غیرممکن است. تنها راه نفوذ به حساب کاربری شما، فریب‌دادن شما تحت عنوان تامین امنیت حساب کاربری و مواردی از این دست است. گول این سودجویان را نخورید.

- **امکاناتی مانند بلوتوث، NFC و ... که برقراری ارتباطات با تلفن همراه را فراهم می‌کنند، فقط در زمان نیاز به استفاده روشن کنید.**

- **مراقب افزونه‌هایی که بر روی برنامه‌های خود نصب می‌کنید، باشید.**

افزونه‌های مرورگرها به تنهایی می‌توانند راهی برای نفوذ و یا جاسوسی از سیستم شما شوند. راه‌حلی قطعی برای اطمینان از امنیت این افزونه‌ها وجود ندارد اما بررسی موارد زیر می‌تواند به مطمئن‌تر شدن شما نسبت به امن‌بودن آن افزونه کمک کند:

- بررسی تعداد نصب آن
- بررسی میزان امتیاز کسب‌شده از جانب کاربران
- بررسی متن توضیحات (ارائه مشخصات کافی از برنامه‌نویس آن و توضیح عملکرد افزونه)
- بررسی کامنت‌های ثبت شده از جانب کاربران

- **از پیام‌رسان‌هایی استفاده کنید که از رمزگذاری End-to-End پشتیبانی می‌کنند.**

در این پیام‌رسان‌ها اطلاعات از جمله چت‌ها در حین ارسال رمزگذاری و در حین دریافت رمزگشایی می‌شوند. کلید رمزگشایی در این ارتباط متغیر است.

- **آنتی‌ویروس معتبر و به‌روز نصب کنید و مرتب آن را به‌روزرسانی کنید.**

لازم به ذکر است که آنتی‌ویروس شما را در مقابل خطرات امنیتی کاملا ایمن نمی‌کند. فقط احتمال ایجاد خطر امنیتی را کاهش می‌دهد.

- **در صورت امکان یک اکانت کاری و یک اکانت شخصی برای سیستم‌عامل خود تعریف کنید یا دو سیستم عامل مجزا در کنار هم برای موارد کاری و شخصی نصب کنید.**

این کار، سبب تضمین امنیت اطلاعات اکانت کاری و یا سیستم‌عاملی که برای موارد کاری اختصاص داده‌اید نمی‌شود، اما امنیت را افزایش می‌دهد.

- **جلسات فعال یا Active Sessions برنامه‌های خود از جمله تلگرام را بررسی کنید. موارد ناشناس و مشکوک را Terminate Access کنید.**

در این قسمت شما می‌توانید دستگاه‌هایی که به حساب کاربری شما متصل هستند را ببینید. اگر پیش‌تر حساب کاربری شما دچار نفوذ فرد دیگری شده باشد، با بررسی این قسمت می‌توانید دستگاه غریبه را تشخیص دهید و دسترسی آن را به حساب کاربری قطع کنید.

- **تلگرام جعلی نصب نکنید!**

پس از فیلتر تلگرام در ایران، تلگرام‌های جعلی و تقلبی بسیاری با نام‌های مختلف منتشر شدند. این پیام‌رسان‌ها از هسته‌ی سرویس متن‌باز تلگرام برای ارائه‌ی امکانات تلگرام استفاده می‌کنند اما تنها نیت پیام‌رسانی را ندارند و در کنار آن، با از دسترسی به گالری تصاویر، مخاطبین و اطلاعاتی دیگر سوءاستفاده و آن‌ها را بدون اطلاع مخاطب به یک سرور دیگر ارسال می‌کنند.

- **در استفاده از ریموت دسکتاپ یا RDP از تنظیمات و پیکربندی‌های امنیتی صحیح اطمینان حاصل کنید.**

معمولا پروتکل ریموت دسکتاپ به طور ذاتی ناامن است و امکان سوءاستفاده را در اختیار سودجویان قرار می‌دهد. در سال‌های اخیر هکرها با نفوذ از طریق این پروتکل و اجرای باج‌افزار در سرور، خسارات زیادی را برای کسب‌وکارها به بار آورده‌اند. به همین دلیل لازم است تنظیمات پیش‌فرض را برای ایجاد امنیت بیشتربا اقداماتی مانند تغییر پورت پیش‌فرض، انتخاب گذرواژه‌ی طولانی و متشکل از کاراکترهای متنوع و ... تغییر دهیم.

- **به برنامه های اندروید معرفی شده در کانال های تلگرام اعتماد نکنید و از نصب آن‌ها خودداری کنید. چون ممکن است جاسوس‌افزار باشند.**

در کانال‌های مختلف تلگرام، ممکن است که با برنامه‌های مختلف اندروید که با عناوین مختلف مذهبی، غیراخلاقی و بهداشتی تبلیغ می‌شوند مواجه شده باشید. این برنامه‌ها به محض نصب بر روی گوشی شما می‌توانند از شما جاسوسی کنند.

- **از اطلاعات مندرج بر روی کارت‌های شناسایی و اعتباری خود محافظت کنید. تصویر آن‌ها را در محل عمومی منتشر نکنید.**

اطلاعات هویتی و بانکی شما به راحتی می‌توانند به روش‌های مختلف توسط هکرها در جهت مهندسی اجتماعی و یا ... برای نفوذ مورد استفاده قرار بگیرند.

در حین کار با سیستم خود:

- **به‌روزرسانی بسیار مهم نرم‌افزارهای خود را به هیچ عنوان به زمانی دیگر موکول نکنید.**

نرم‌افزارهای مورداستفاده در سیستم خود را به‌روزرسانی کنید و در صورت ارائه‌ی وصله‌ی امنیتی یا Patch برای هرکدام، آن را در اسرع وقت نصب کنید؛ چراکه معمولا در نسخه‌های جدید، نقص‌های موجود در نسخه‌ی قبلی رفع و نفوذ برای نفوذگر سخت‌تر می‌شود.

- **کارهای مهم خود را با اتصال به وای‌فای عمومی و نامطمئن انجام ندهید.**

استفاده از شبکه‌های ناایمن و عمومی، این امکان را مهیا می‌سازد که مهاجمین بتوانند با زیرنظرداشتن ترافیک اینترنت شما، به اطلاعات ارزشمندی دست یابند. در موارد ضروری حتما برای ارتباطات و در سامانه‌های خود از ارتباطات شبکه‌ای رمزگذاری‌شده به ویژه از پروتکل HTTPS استفاده کنید.

در سامانه‌های کاری خود:

- **فایل‌های حساس و محرمانه‌ای مانند اطلاعات مشتریان را به صورت رمزگذاری‌شده جابه‌جا یا ارسال کنید.**

رمزگذاری باعث می‌شود تنها مخاطب موردنظر شما که کلید رمزگشایی را در اختیار دارد، بتواند فایل را باز کند.

- **در دورکاری احتمال تبادل اطلاعاتی مانند گذرواژه‌های حساب‌های کاربری کاری و غیرکاری مابین اعضای دورکار بالاست. تا حد امکان از تبادل این اطلاعات در محیط‌هایی نظیر پیام‌رسان‌ها پرهیز کنید یا در صورت لزوم تبادل، پس از انجام کار موردنظر گذرواژه را تغییر دهید.**

چراکه اگر این اطلاعات در جریان جابه‌جایی بر حسب تصادف و یا مورد نفوذ قرارگرفتن در دسترس افراد سودجو قرار گیرند، امکان دسترسی آن افراد به حساب کاربری را فراهم می‌کنند نوشتن آدرس‌های مهم از جمله آدرس پست الکترونیکی و شماره تلفن و یا موارد دیگر، در حالت کلی موردی ندارد اما باید توجه داشته باشید که اغلب، این اطلاعات محرمانه به شمار می‌آیند و یادداشت آن‌ها چه به صورت مجازی و چه به صورت حقیقی باید موقتی باشد و پس از اتمام

کار حذف شوند. می‌توانید محض اطمینان ابتدای محتوای تبادل‌شده عبارتی با مضمون "بعدا حذف شود" را اضافه کنید تا در اسرع وقت آن اطلاعات را حذف کنید تا محرمانگی نقض نشود.

- **از گذرواژه‌ها و اطلاعات حساس کاربری خود مراقبت کنید.**

گذرواژه‌ی خود را در وهله‌ی اول با هیچ‌کس به اشتراک نگذارید. اگر مجبور به اشتراک‌گذاری آن شدید، پیش از آن از مورد اعتمادبودن همکار خود اطمینان کامل حاصل کنید.

- **از گذرواژه‌های بلند و متشکل از حرف و عدد استفاده کنید.**

هر چه طول گذرواژه انتخابی شما بیشتر و متشکل از کاراکترهای متنوع‌تری باشد، حدس گذرواژه‌ی شما سخت‌تر و در حملاتی نظیر Bruteforce احتمال موفقیت هکر برای نفوذ به حساب کاربری شما کم‌تر می‌شود.

- **از گذرواژه‌های یکسان برای حساب‌های کاربری مختلف خود استفاده نکنید.**

اگر شما در همه‌ی سامانه‌هایی که در آن‌ها عضو هستید، از یک گذرواژه‌ی یکسان استفاده کرده باشید. با نشت اطلاعات هر کدام از آن سامانه‌ها، گذرواژه‌ی شما افشا می‌شود و هکر می‌تواند با امتحان‌کردن آن گذرواژه در سامانه‌های دیگری که شما عضو هستید، به درون آن سامانه‌ها نفوذ و به آن‌ها دسترسی پیدا کند.

- **برای انتخاب و سامان‌دهی گذرواژه‌های خود، از برنامه‌های مدیریت گذرواژه استفاده کنید.**

این برنامه‌ها، گذرواژه‌ای تصادفی برای شما تولید و نگه‌داری می‌کنند تا در همه‌ی سیستم‌های خود برای فرار از فراموشی از یک گذرواژه‌ی یکسان استفاده نکنید.

- **به طور منظم از اطلاعات حساس خود بکاپ بگیرید.**

با استفاده از یک نرم‌افزار بکاپ از فایل‌های مهم، پشتیبان تهیه و خارج از فضای اینترنت نگه‌داری کنید تا در صورت رخ‌دادن حمله‌ی باج‌افزاری و یا سرقت آن‌ها از طریق نفوذ به سامانه، قابلیت بازیابی داده‌ها وجود داشته باشد.

در جلسات و هم‌کاری‌های خود:

- **در مواقعی که از وب‌کم دستگاه خود استفاده نمی‌کنید، آن را با تکه‌ای کاغذ بپوشانید و یا به صورت نرم‌افزاری مسدود کنید.**

در صورتی که وب‌کم به صورت پیش‌فرض آزاد باشد، احتمال سوءاستفاده از آن توسط هکر و به کمک ابزارهای جاسوسی بالا می‌رود. به عنوان نمونه، هکر می‌تواند با ضبط تصویر وب‌کم از شما اخاذی کند و یا شما را وادار به جاسوسی در سازمان کند.

- **به کمک استفاده از ابزار یا لوازم جانبی مانع دیده‌شدن صفحه نمایش خود از زوایای دیگر شوید.**

افرادی که مجاز نیستند محتوای محرمانه‌ای که در صفحه‌ی نمایش دیده می‌شود را ببینند، قادر خواهند بود که با مشاهده‌ی تصویر نمایش‌گر و مواردی که شما تایپ می‌کنید، به اهداف خود در جمع‌آوری اطلاعات که یک مرحله از فرآیند نفوذ است، برسند.

- **دستگاه‌های خود را در اختیار کودکان و اعضای دیگر خانواده قرار ندهید.**

ممکن است آن‌ها اطلاعات مهمی که شما در دستگاه‌های خود دارید، به طور اتفاقی به افراد دیگر ارسال کنند و شما هیچ‌گاه متوجه این اتفاق نشوید.

- **هیچ‌گاه دستگاه خود را به ویژه حین تماس یا جلسه‌ی کاری قفل‌نکرده، ترک نکنید. قفل خودکار سیستم‌عامل را فعال کنید.**

هرکدام از ما به نوبه‌ی خود فراموش‌کار هستیم. رهاکردن سیستم به صورت قفل‌نشده خطر سوءاستفاده افراد دیگر در آن محل را بالا می‌برد.

- **زمانی که در جلسه صفحه‌نمایش خود را به اشتراک می‌گذارید، مراقب باشید که اطلاعات محرمانه را باز نکنید، از انتشار نماهایی از لیست برنامه‌های نصب‌شده بر روی سیستم خودداری و هنگام وارد نمودن اطلاعات ورود (نام کاربری و گذرواژه) در سامانه‌ها احتیاط کنید.**

آگاهی هکر از نرم‌افزارهای مورداستفاده‌ی شما، به او در جمع‌آوری اطلاعات و ایده‌پردازی در جهت پیداکردن راه نفوذ کمک می‌کند.

- **در تبادل و نقل‌وانتقال فایل‌ها با مشتریان و همکاران احتمال وجود خطر بدافزار در آن‌ها را در نظر بگیرید و پیش از استفاده آن‌ها را اسکن کنید.**

اگر منتظر دریافت فایل یا لینک از طرف مشتریان یا همکاران خود هستید، به امنیت آن فایل و لینک خوش‌بین نباشید. به عنوان نمونه فایل اسنادی مانند Word، Excel و PDF می‌تواند با ماکرو همراه باشند؛ در واقع هکر کد بدخواهانه‌ی خود را در ماکرو نوشته باشد و با بازکردن این فایل‌ها، آن کد خودبه‌خود بر روی سیستم اجرا شود. حتی امکان دارد که خود ارسال‌کننده نیز از وجود بدافزار و خطر آن فایل یا لینک آگاه نباشد و خود نیز پیش‌تر این فایل یا لینک مخرب را از فرد یا سایت دیگری دریافت کرده باشد. در این مواقع می توانید صحت فایل‌ها و لینک‌ها را در سایت https://virustotal.com بررسی کنید.

اگر مسئول آی‌تی یا امنیت هستید:

- **باید بدانید که تعطیلات زمان شدت‌گرفتن جولان هکرها، بدافزارها و به ویژه باج‌افزارها است. بهتر است در این ایام، بسیار هوشیار باشید و به طور مداوم به دنبال کشف فعالیت مشکوک باشید.**

در موقعیت‌هایی که وضعیت سفید نیست و احتمال خطر وجود دارد، به طور مرتب ترافیک شبکه را زیر نظر داشته و به دنبال کشف فعالیت‌های مشکوک باشید.

- **در مواقع وقوع حادثه در صورت نیاز به اطلاع‌رسانی، با توجه به اهمیت بالای موضوع از تماس تلفنی برای ارتباط با مدیر ارشد خود استفاده کنید. از برنامه‌هایی مانند واتس‌اپ و پیام رسان‌های دیگر که امنیت کمتری دارند فقط برای ارتباطات فوری استفاده کنید.**

در موقعیت‌هایی که وضعیت سفید نیست و احتمال خطر وجود دارد، اطلاع‌رسانی به‌موقع می‌تواند در کنترل شرایط بسیار موثر باشد. دقت کنید که در چنین موقعیتی تنها در صورت اضطرار از پیام‌رسان‌های عمومی جهت انتقال فوری پیام استفاده کنید. چون کنترل محرمانگی در این پیام‌رسان‌ها سخت‌تر است و در حالت عادی بهتر است از این پیام‌رسان‌ها استفاده نشود.

- **نسخه‌ای چاپ شده از دستورالعمل‌ها و چک‌لیست‌های امنیتی لازم در دورکاری برای پوزیشن کاری خود را تهیه کنید و اطمینان حاصل کنید که آن نسخه توسط افرادی غیر از خودتان به سادگی قابل دست‌یابی نیست.**

کارهای خود را به صورت فرآیندی و موردی یادداشت و در جای ایمن و مطمئنی نگه‌داری کنید تا در هر بار انجام کار، تمام اصول چک‌لیست را به ترتیب بررسی کنید. گاهی فراموشی یک اصل امنیتی منجر به خسارت‌های جبران‌ناپذیری می‌شود. در صورتی که محرمانگی این دستورالعمل‌ها حفظ نشود، امکان دارد مهاجم به هر روشی به فناوری‌های استفاده‌شده در مجموعه‌ای که در آن کار می‌کنید، پی ببرد. این اطلاعات، قطعا برای هکر در فرآیند نفوذ ارزش‌مند خواهند بود.

- **تا حد امکان از خدمات ذخیره‌سازی ابری خارجی برای کارهای خود استفاده نکنید. در صورت تمایل به استفاده، با مدیر ارشد خود مشورت کنید.**

بهتر است که از این سرویس‌ها استفاده نشود اما در صورت لزوم، از سرویسی استفاده کنید که شرایط احراز هویت آن مطمئن باشد و از احراز هویت دو مرحله‌ای نیز پشتیبانی کند.

- **برای امنیت بیشتر و کاهش خطر نشت اطلاعات از Access Control برای افراد دورکار استفاده کنید.**

محدودیت‌هایی اعمال کنید که فقط افرادی که شما مشخص می‌کنید تا سطح مشخصی به سرویس‌های محرمانه دسترسی داشته باشند.

- **برای کار با سامانه‌ها VPN راه‌اندازی کنید و برای هر فرد دورکار یک حساب کاربری ایجاد کنید.**

با این کار، ارتباط خصوصی‌تری نسبت به ارتباط بر بستر اینترنت ایجاد و امنیت بیشتری برای ارتباطات افراد دورکار با سامانه فراهم می‌شود.

روز و روزگارتون امن ؛)