توصیه‌ها و الزامات رعایت امنیت در دورکاری

منبع: تیم پاسخگویی واکنش سریع رایانه‌ای (CERT) سازمان همکاری‌های اسلامی

۱- آماده‌سازی محل کار اختصاصی در منزل

a. ترجیحاً محل کاری اختصاصی، امن و ایزوله برای کار در منزل داشته باشید
b. اطمینان حاصل کنید فضا برای نگهداری وسایل و اسناد سازمانی مناسب است
c. انتظارات خود از اطرافیانتان را به درستی تنظیم کنید
d. سازماندهی درستی انجام دهید تا دچار از دست‌دادن داده‌ها نشوید
e. لباس مناسب داشته و برای تماس‌های غیرمنتظره تصویری آماده باشید

۲- امنیت فیزیکی

a. از حفاظت فیزیکی وسایل سازمانی یا هر وسیله حاوی داده‌های سازمانی اطمینان حاصل کنید
b. راه‌کارهای حفاظتی مناسب برای مواردی مانند گرما، گرد و غبار و سرقت اتخاذ کنید
c. فایل‌های سازمانی را از دسترس کودکان و حیوانات خانگی دور نگهداری کنید

۳- برای حفاظت از آن، قفلش کنید

a. رایانه خود را در صورتی‌که از آن دور می‌شوید قفل کنید (در ویندوز با فشردن کلیدهای Windows+L)
b. اگر از مکان عمومی کار می‌کنید مراقب نگاه‌کردن دیگران از روی شانه خود باشید

٤- از به اشتراک‌گذاری اجتناب کنید

a. وسایل سازمانی مانند رایانه و لپ تاپ را با اعضای خانواده یا دوستان به اشتراک نگذارید
b. هرگز داده‌های طبقه بندی شده سازمانی را با افراد غیرمجاز به اشتراک نگذارید

۵- از استفاده شخصی خودداری کنید

a. از وسایل سازمانی تنها برای کارهای مرتبط با سازمان استفاده کنید
b. از نصب نرم‌افزارهایی که مرتبط با کار سازمان نیستند خودداری کنید
c. فلش مموری‌های شخصی خود را به کامپیوتر سازمانی متصل نکنید

۶- امنیت رایانامه

a. از رایانامه (ایمیل) شخصی برای کارهای سازمانی استفاده نکنید
b. از رمزگذاری end-to-end استفاده کنید (با فعالسازی S/MIME در بخش تنظیمات)
c. استفاده از امکان پاسخ به همه "reply-to-all" را محدود کنید
d. روی پیوندهای مشکوک در رایانامه‌های دریافتی کلیک نکنید، حتی اگر آن را از یک منبع آشنا دریافت کرده باشید
e. همیشه قبل از پاسخ دادن، فرستنده را اعتبارسنجی کنید
f. پیوست‌های رایانامه را برای اطمینان از نداشتن ویروس و بدافزار، اسکن کنید

۷- استفاده از اتصال امن

a. تنها با استفاده از راهکار تایید شده سازمان، به شبکه سازمانی متصل شوید
b. از شبکه‌های بی‌سیم عمومی برای انجام کارهای سازمانی استفاده نکنید
c. شبکه بی‌سیم خانگی خود را امن‌سازی کنید
d. به اتصال‌های ناامن بی‌سیم متصل نشوید

۸- امن‌کردن شبکه بی‌سیم خانگی:

a. تنظیمات بی‌سیم خانگی خود را از از تمام دستگاه های متصل به آن (رایانه، لپ تاپ، گوشی و ...) حذف کنید و تغییرات زیر را در روتر بی‌سیم (مودم) خود انجام دهید:
   i. مطمئن شوید firmware آن به‌روز است. اگر قدیمی باشد در تنظیمات آن نشان داده می‌شود.

ii. یک نام یا SSID منحصربه‌فرد برای آن انتخاب کنید

iii. SSID را مخفی کرده و یک شبکه مخفی بسازید

iv. یک رمز عبور منحصربه‌فرد و قوی بسازید

v. برای قوی‌ترکردن امنیت از پروتکل WPA۲ یا WPA۳ استفاده کنید

۹- اولین خط دفاعی (رمز عبور) خود را مستحکم کنید

a. با یک جمله رمز شروع کنید I Love Chocolate

b. برخی حروف را با ارقام جایگزین کنید ۱ L۰v۳ Ch۰c۰lat۳

c. برخی حروف را با کاراکترهای خاص جایگزین کنید ۱ L۰v۳ C#۰c۰l@t۳

d. برخی حروف را کوچک و برخی را بزرگ استفاده کنید ۱l۰V۳c#۰C۰L@t۳

۱۰- شناسه‌های خود را به اشتراک نگذارید

a. رمزعبور خود را با دوستان و اعضای خانواده به اشتراک نگذارید

b. رمز عبور خود را یادداشت نکنید

c. برای اکانت‌های مختلف از رمز عبور مشابه استفاده نکنید

۱۱- استفاده از اعتبارسنجی دو عاملی

a. برای ایجاد لایه محافظتی اضافه، از اعتبارسنجی دو یا چند عاملی استفاده کنید

b. به عنوان مثال: اعتبارسنجی با ایمیل یا پیامک، توکن امن تصادفی، روش‌های بیومتریک مانند تشخیص چهره یا اثر انگشت و غیره

۱۲- ویدیو کنفرانس

a. تنها از ویدیو کنفرانس‌ها، بسترها و ابزار به اشتراک‌گذاری اطلاعات مطمئن و تایید شده سازمانی استفاده کنید.

b. از ابزارهای همکاری سازمانی، استفاده شخصی نکنید

۱۳- همکاری آنلاین

a. قبل از به اشتراک‌گذاری فایل‌ها، آنها را با ابزارهای به‌روز ضد بدافزار، اسکن کنید

b. فایل‌هایی که منبع نامشخص دارند به اشتراک نگذارید

c. هیچ دعوتی را از سوی کاربران ناشناخته نپذیرید

d. هرگونه فعالیت مشکوک را بلافاصله به مدیر سیستم اطلاع دهید

e. بدون اجازه تمام طرف‌های مشارکت‌کننده، از مباحثات مطرح شده عکس یا فیلم نگیرید

f. در جلساتی که نیازمند فعال‌بودن وب‌کم هستند، استانداردهای پوشش سازمانی را رعایت کنید

۱۴- امن‌سازی ابزارهای همکاری

a. اتاق‌های انتظار را فعال کنید

b. برای ملحق شدن به اتاق‌ها، رمز عبور را اجباری کنید

c. از شناسه جلسه شخصی استفاده نکنید

d. جلسه را قفل کنید

e. تبادل فایل را ببندید

f. به اشتراک‌گذاری صفحه فقط در اختیار میزبان جلسه باشد

۱۵- استفاده از برنامه‌های کاربردی ابری تایید شده

a. از آنجا که در استفاده از فضای ابری، داده‌های سازمانی در فضای ابری ذخیره می‌شوند، این ابزار حتماً باید مورد تایید سازمان باشد تا داده‌ها تنها در اختیار افراد مجاز قرار داشته باشد

۱۶- دانلود برنامه‌های کاربردی تایید شده

a. کارکنان بایستی نصب هرگونه برنامه کاربردی را به واحد مربوطه اطلاع دهند

b. به ازای هر دانلود باید تاییدیه گرفته شود

۱۷- مراقب کلاه‌برداری باشید

a. کلاه‌برداری‌ها از طریق مهندسی اجتماعی: بازی با تمایل طبیعی انسان به سمت اعتماد. از قربانیان خواسته می شود اطلاعاتی را ارائه و یا اقدامی انجام دهند.

b. کلاه‌برداری فیشینگ: مهندسی اجتماعی از طریق رایانامه به صورتی که هکر سعی می‌کند با ارسال رایانامه‌هایی که ظاهراً از مراجع معتبر ارسال شده‌اند، کاربران را فریب دهد

c. از سایر ابزارهای ارتباطی مانند پیامک، تلفن، ابزار ویدیو کنفرانس، شبکه‌های اجتماعی و غیره نیز برای فریب استفاده می‌شود

۱۸- مراقب حملات سایبری باشید

a. مراقب حملات فیشینگ به کاربران با اطلاعات مرتبط به ویروس کوئید ۱۹ (کرونای جدید) باشید

b. هرگز روی پیوندها یا پیوست‌های فایل در رایانامه‌های مشکوک کلیک نکنید و آن‌ها را به مدیر سیستم اطلاع دهید

۱۹- تبادل اطلاعات

a. از کانال‌های تایید شده سازمان برای تبادل و انتقال فایل‌ها استفاده کنید

b. بر اساس سطح طبقه‌بندی اطلاعات از کانال ارتباطی مناسب برای به اشتراک‌گذاری یا تبادل فایل استفاده کنید

c. از درایو به اشتراک‌گذاری شده سازمانی برای نگهداری اطلاعات استفاده کنید تا امکان پشتیبان‌گیری از داده‌ها فراهم باشد و اطلاعات از دست نرود

۲۰- به طور منظم به‌روزرسانی‌ها را نصب کنید

a. به اعلان‌های یادآوری برای به‌روزرسانی نرم‌افزارها توجه کنید

b. دستگاه خود را به گونه‌ای تنظیم کنید که به صورت خودکار به‌روز شود

۲۱- امن‌سازی ابزار شخصی

a. سیستم‌عامل و نرم‌افزار خود را به صورت منظم به‌روزرسانی کنید

b. از نرم‌افزار مورد اطمینان و به‌روز ضد بدافزار استفاده کنید

c. داده های خود را در محل مطمئنی پشتیان‌گیری کنید

d. تنها از منابع مورد اطمینان، نرم‌افزار دریافت و نصب کنید

e. از یک فایروال دسکتاپ استفاده کنید

۲۲- مطابق سیاست‌ها و روال‌های سازمان عمل کنید

a. سیاست‌ها و روال‌های سازمان برای دورکاری را مطالعه کرده و از آن‌ها تبعیت کنید

۲۳- گزارش رخدادها

a. هرگونه رخداد امنیت اطلاعات را به پشتیبانان فاوا اطلاع دهید

b. رخدادهای امنیتی شخصی را به مقامات ذیربط اطلاع دهید