Committee to Protect Journalists

بسته (کیت) ایمنی دیجیتال

روزنامه‌نگاران باید با به روز نگه‌داشتن اطلاعات خود درباره‌ی آخرین اخبار حوزه‌ی امنیت دیجیتال و تهدیداتی مانند هک کردن، فیشینگ و نظارت، از خود و منابع خبری خود محافظت کنند. روزنامه‌نگاران باید درباره‌ی اطلاعاتی که در اختیار دارند تامل کنند و در نظر بگیرند که اگر این اطلاعات به دست افراد نادرست بیفتد چه پیامدهایی می‌تواند به دنبال داشته باشد و پس از در نظر گرفتن این امر، اقدامات لازم در راستای حفاظت از حساب‌ها، دستگاه‌ها، ارتباطات و فعالیت‌های آنلاین (برخط) خود انجام دهد.

فهرست

Committee to Protect Journalists

از حساب‌های کاربری خود محافظت کنید

روزنامه‌نگاران از حساب‌های کاربری مختلفی در فضای مجازی استفاده می‌کنند که حاوی اطلاعات شخصی و کاری خود، خانواده، همکاران و منابع خبری‌شان است. شما می‌توانید با تضمین امنیت این حساب‌ها، پشتیبانی گرفتن و حذف اطلاعات به طور مداوم، از خود در برابر هکرها محافظت کنید. برداشتن این قدم‌ها بویژه برای آن دسته از روزنامه‌نگارانی اهمیت دارد که ممکن است هدف دشمنی افرادی با توانمندی تکنولوژیکی بالا قرار گیرند.

برای محافظت از حساب‌های کاربری خود:

- در نظر بگیرید چه اطلاعاتی درحساب‌های مختلف شما ذخیره شده و اگر حسابتان هک شود، چه خطرات و پیامدهایی برای خود، خانواده و منابع خبری شما در پی خواهد داشت.
- تنظیمات حریم خصوصی خود را بررسی کنید تا بدانید کدام بخش از اطلاعاتتان، بویژه در رسانه‌های اجتماعی، برای همه افراد قابل مشاهده است.
- از تمام اطلاعات حساس و یا اطلاعاتی که نمی‌خواهید در دسترس عموم قرار گیرد، به ویژه پیام‌های خصوصی خود، پشتیبانی گرفته و بعد آنها را از روی گوشی و داخل حساب‌های کاربری خود پاک کنید. نسخه‌های کپی شده را روی یک هارد خارجی یا در حساب ابری (cloud) ذخیره کنید.
- حساب‌هایی را که دیگر استفاده نمی کنید، پاک کنید. قبل از پاک کردن حتما از اطلاعاتی که می‌خواهید نگه‌داری کنید، نسخه پشتیبان تهیه کنید.

- برای حساب‌های خود از گذرواژه‌های منحصر بفرد و طولانی استفاده کنید. از هیچ گذر واژه‌ای بیش از یکبار استفاده نکید. برای مدیریت گذرواژه‌هایتان از نرم‌افزار مدیریت گذرواژه استفاده کنید.

- از تایید هویت دو مرحله‌ای (FA2) و در صورت امکان از یک کلید امنیتی نظیر Yubikey استفاده کنید.

- بطور مرتب از بخش آخرین فعالیت حساب خود بازبینی کنید. با این کار اگر دستگاهی که نمی شناسید به حسابتان وصل شده باشد، مطلع می شوید.

Committee to Protect Journalists

فیشینگ

اغلب روزنامه‌نگاران یک پروفایل عمومی دارند و اطلاعات تماس خود را برای گرفتن سرنخ از منابع خبری، به اشتراک می گذارند. دشمنانی که به دنبال دستیابی به داده‌ها و دستگاه‌های روزنامه‌نگاران هستند، می‌توانند با حملات فیشینگ فرد روزنامه‌نگار یا یکی از اقوام و همکارانش را مورد هدف قرار دهند. حملات فیشینگ ممکن است در قالب نامه الکترونیکی، پیام کوتاه، پیام در رسانه‌های اجتماعی یا پیام‌رسان‌ها باشد و طوری طراحی شده‌اند تا گیرنده را برای به اشتراک گذاشتن اطلاعات حساس یا کلیک روی پیوند یا دانلود فایل حاوی بدافزار، فریب دهند. تنوع و درجه‌ی پیچیدگی بدافزارها و جاسوس‌افزارها زیاد است. پیشرفته‌ترین آنها به مهاجمان دسترسی کامل به دستگاه و تمام محتوای آن را می‌دهد.

برای پیشگیری از حملات فیشینگ:

- درباره‌ی توانمندی تکنولوژیکی دشمنان خود تحقیق کنید تا بفهمید شما یا آشنایان‌تان تا چه حد در معرض خطر قرار دارید.

- به پیام‌هایی که به شما توصیه می‌کنند کاری را به سرعت انجام دهید و یا پیشنهادی می‌دهند که بیش از اندازه‌ی معقول خوب به نظر می‌رسد، شک کنید. مخصوصا اگر لازم باشد روی پیوندی کلیک کرده یا یک فایل ضمیمه را دانلود کنید.

- جزئیات حساب فرستنده و محتوای پیام را با دقت بررسی کنید تا از صحت آن اطمینان حاصل کنید. تغییرات کوچک در املا، دستور زبان، محتوا و یا لحن ممکن است نشانگر آن باشد که حساب اسپوف (جعلی) یا هک شده است.

- اگر پیام حاوی مطلب مشکوک یا عجیبی بود، با استفاده از یک روش جایگزین مانند تماس تلفنی صحت و سقم پیام را با فرستنده‌ی آن تایید کنید.

- قبل از کلیک بر روی پیوندها تامل کنید، حتی اگر به نظر می‌رسد فرستنده‌ی پیام را می‌شناسید. به مدت چند ثانیه مکان‌نمای خود را روی پیوند نگه داشته تا آدرس URL ظاهر شود و قبل از کلیک کردن از درستی آن اطمینان حاصل کنید.

- پیش نمایش فایل‌های ضمیمه‌ی پست الکترونیکی را مشاهده کنید. اگر فایل آلوده را دانلود نکنید، بدافزار همانجا می‌ماند و در سیستم شما پخش نمی‌شود. اگر شک دارید، با ارسال‌کننده‌ی فایل تماس بگیرید و از او بخواهید محتوای فایل ضمیمه را در متن پست الکترونیکی کپی کند.

- پیوندها و فایل‌های مشکوک را در تارنمای رایگان ویروس توتال (Virus Total) بارگذاری کرده و از نظر آلوده نبودن به بدافزار بررسی کنید. البته این تارنما تنها ویروس‌های شناخته شده را پیدا می‌کند.

- به روز رسانی خودکار را فعال کنید تا نرم‌افزارهای دستگاه‌هایتان همواره به روز باشند. این کار شکاف‌هایی را که بدافزارها از آن برای ایجاد خطر امنیتی استفاده می‌کنند، برطرف می‌کند.

- نسب به حملات فیشینگ هوشیار باشید به ویژه در زمان انتخابات، ناآرامی و یا اگر همکاران و اعضای جامعه مدنی محلی اظهار کردند که مورد هدف قرار گرفته‌اند.

امنیت دستگاه

روزنامه‌نگاران برای تولید و ذخیره‌ی محتوای مطالب و تماس با منابع خبری خود، از دستگاه‌های متنوعی استفاده می‌کنند. بسیاری از روزنامه نگاران، به ویژه روزنامه نگاران آزاد، چه در خانه و چه در محل کار از یک دستگاه استفاده می‌کنند که در صورت گم شدن، سرقت و یا ضبط این دستگاه، حجم زیادی از اطلاعات‌شان در معرض خطر قرار می‌گیرد. هارد رایانه، گوشی همراه، تبلت و هاردهای خارجی خود را مخصوصا قبل از سفر، رمزگذاری کرده تا مطمئن شوید کسی بدون داشتن گذرواژه قادر به دسترسی به اطلاعات‌تان نخواهد بود.

برای ایمن سازی دستگاه‌های خود:

- دستگاه‌های خود را با گذرواژه، کد، یا رمز عبور قفل کنید. هک کردن رمزهای عبور یا گذرواژه‌های طولانی‌تر، دشوارتر است.

- هر زمان اعلان بروزرسانی سیستم عامل دریافت کردید، نسبت به نصب آن اقدام کرده تا از دستگاه‌های خود در برابر آخرین بدافزارها محافظت کنید.

- اطلاعات ذخیره شده در دستگاه‌های خود را بررسی کنید و در نظر بگیرید کدام یک از آنها می‌تواند شما یا دیگران را در معرض خطر قرار دهد.

- بطور مرتب از دستگاه‌های خود نسخه پشتیبان تهیه کنید تا در صورت از بین رفتن، گم شدن یا سرقت دستگاه، اطلاعات خود را از دست ندهید. نسخه‌های پشتیبان را در جایی امن و دور از محل کار معمول خود ذخیره کنید.

- اطلاعات حساس مانند پیام‌های متنی را به طور مرتب حذف کنید. برای جلوگیری از بازیابی مجدد پرونده‌های حذف شده توسط دیگران، در صورت امکان از نرم افزار پاکسازی اطلاعات استفاده کنید، در غیر این صورت دستگاه را به تنظیمات کارخانه بازگردانده و از آن برای فعالیت‌های غیر مرتبط استفاده کنید تا حافظه دستگاه بازنویسی شود. (قبل از این کار از هر چه می خواهید حفظ کنید، نسخه‌ی پشتیبان تهیه کنید وگرنه اطلاعاتتان از دست می‌رود.)

- در اماکن عمومی دستگاه‌های خود را بدون نظارت رها نکنید، حتی هنگام شارژ کردن، چون ممکن است به سرقت رفته و یا دستکاری شوند.

- دستگاه‌های خود را به درگاه‌های USB عمومی وصل نکنید یا از فلش مموری‌هایی (USB) که در مراسم مختلف هدیه داده می‌شوند، استفاده نکنید . این فلش‌ها ممکن است حاوی بدافزار باشند و رایانه‌ی شما را آلوده کنند.

- دقت کنید که دستگاه شما ممکن است نسخه‌ی پشتیبان اطلاعاتتان را در حساب ابری متصل به شماره تلفن، ذخیره کند. اطلاعات ذخیره شده در حساب ابری ممکن است رمزگذاری شده نباشند. می‌توانید گزینه پشتیبان‌گیری خودکار را در تنظیمات گوشی غیرفعال کنید.

- دستگاه‌های خود را از قبل طوری تنظیم کنید تا در صورت سرقت، بتوانید داده‌های روی آن را از راه دور پاک کنید. توجه کنید که دستگاه تنها در صورت اتصال به اینترنت پاک می‌شود.

- همیشه تعمیر دستگاه‌های خود را به یک تعمیرگاه معتبر بسپارید.

Committee to Protect Journalists

برای رمزگذاری دستگاه خود:

- تلفن‌های هوشمند جدیدتر قابلیت رمزگذاری دارند، فقط از روشن بودن این قابلیت در تنظیمات گوشی مطمئن شوید.

- برای فعال کردن رمزگذاری کامل دیسک در ویندوز از Bitlocker ، در سیستم مک از Firevault ، و از نرم افزار رایگان Veracrypt برای هاردها و دستگاه‌های ذخیره خارجی استفاده کنید.

- لازمه‌ی استفاده از رمزگذاری، انتخاب گذرواژه‌های طولانی و منحصر بفرد است. در گوشی‌های هوشمند، برای افزودن گذرواژه‌ی طولانی‌تر و پیچیده‌تر به بخش تنظیمات سفارشی رجوع کنید.

- دقت کنید که فردی که گذرواژه‌ی شما را می‌داند یا می‌تواند شما را به رمزگشایی دستگاه‌تان وادار کند، قادر به دیدن اطلاعاتتان خواهد بود.

- مطمئن شوید رمزگذاری در کشوری که در آن زندگی می‌کنید یا قصد سفر به آن را دارید، قانونی است.

ارتباطات رمزگذاری شده

روزنامه‌نگاران می‌توانند با استفاده از برنامه‌های پیام‌رسان رمزگذاری شده، یا نرم‌افزارهای رمزگذار پست الکترونیکی که فقط برای گیرنده مد نظر مطالب را رمزگشایی می‌کنند، با امنیت بیشتری با منابع خود ارتباط برقرار کنند. استفاده از برخی ابزارها راحت‌تر از بقیه است. رمزگذاری از محتوای پیام‌ها محافظت می‌کند. اما شرکت‌های تولید کننده‌ی این نرم‌افزارها باز هم می‌توانند فراداده (متادیتا) را مشاهده کنند که شامل اطلاعاتی مانند زمان ارسال پیام، فرد دریافت کننده‌ی پیام، و سایر جزییات آشکارکننده‌ی هویت شما است. سیاست شرکت‌های نرم‌افزاری درباره‌ی نحوه‌ی ذخیره‌ی این داده‌ها متفاوت است. این شرکت‌ها رویکردهای مختلفی در قبال تحویل این نوع داده‌ها به مسئولان دارند.

برنامه‌های پیام‌رسان خوب، رمزگذاری سراسری دارند به این معنی که اطلاعات هنگام ارسال از فرستنده به گیرنده رمزگذاری می‌شود. فرستنده و گیرنده هر دو باید از یک اپلیکیشن استفاده کنند. البته هر فردی که دستگاه فرستنده یا گیرنده‌ی پیام، و یا گذرواژه‌ی آن اپلیکیشن را در اختیار داشته باشد، می‌تواند به محتوای پیام دست یابد. سیگنال، واتساپ و تلگرام چند برنامه‌ی پیام‌رسان با رمزگذاری سراسری هستند.

ایمیل رمزگذاری شده راهی امن‌تر برای تبادل اطلاعات با منابع خبری یا مخاطبان است. برای ارسال و دریافت ایمیل رمزگذاری شده، هر دو طرف باید نرم افزار خاصی را دانلود و نصب کنند.

برای استفاده از برنامه‌های پیام‌رسان رمزگذاری شده:

- تحقیق کنید صاحب اپلیکیشن کیست، چه اطلاعاتی را ذخیره می‌کند و آیا تاکنون دولتی برای دریافت این اطلاعات حکم قضایی صادر کرده است؟ ببینید سیاست آنها در قبال درخواست به اشتراک‌گذاری داده‌های کاربران چیست.

- در صورت امکان، برای اپلیکیشن از رمزعبور یا گذرواژه استفاده کنید تا اگر گوشی دزدیده شد، کسی نتواند آن را باز کند.

- ببینید اطلاعات ارسال شده به برنامه‌های پیام‌رسان در کجای تلفن همراه‌تان ذخیره می‌شود.

- هرچیزی که دانلود کنید، مانند عکس، در دستگاه شما ذخیره می‌شود و می‌تواند روی دستگاه‌ها و اپلیکیشن‌های دیگر کپی شود مخصوصا هنگامی که از داده‌های خود نسخه‌ی پشتیبان تهیه می‌کنید.

- برخی برنامه‌ها مانند واتساپ از پیام‌های شما در حساب ابری متصل به شماره تلفن، نسخه‌ی پشتیبان تهیه می‌کنند.

- مخاطبین ذخیره شده در تلفن همراه شما با برنامه‌های پیام‌رسان و حساب‌های ابری همگام سازی می‌شوند، بنابراین شماره تلفنی را که در یک جا پاک کرده‌اید ممکن است در جایی دیگر همچنان موجود باشند.

- بطور مرتب از پیام‌های خود نسخه پشتیبانی گرفته و آنها را پاک کنید تا کمترین اطلاعات ممکن در دستگاه یا حساب کاربری ذخیره شده باشد. برای بررسی محتوا، از جمله اسناد و پیام‌های چندرسانه‌ای، فرایندی در نظر بگیرید و دانلودها و اسکرین‌شات‌های (نما گرفت) خود را روی یک هارد (حافظه) خارجی رمزگذاری شده، ذخیره کنید.

- گزینه‌ی ارسال پیام‌های ناپدید شونده در سیگنال به شما امکان این امکان را می دهد تا پیام‌ها را پس از مدت زمان معینی به طور خودکار حذف کنید.

برای استفاده از ایمیل رمزگذاری شده:

- از آشنای قابل اعتمادی که دانش فنی دارد کمک بگیرید. ممکن است نصب پست الکترونیکی رمزگذاری شده برای افراد تازه کار ساده نباشد.

- نرم افزاری برای رمزگذاری پست الکترونیکی انتخاب کنید که معتبر و بررسی شده باشد. برای محافظت در برابر شکاف‌های امنیتی همواره نرم‌افزار خود را به روز رسانی کنید.

- از قبل برای نرم‌افزار رمزگذار پست الکترونیکی خود گذرواژه‌ای طولانی و منحصر به فرد انتخاب کنید. اگر این گذرواژه را فراموش کنید، دیگر به نامه‌های الکترونیکی رمزگذاری شده‌ی خود دسترسی نخواهید داشت.

- بطور مرتب نامه الکترونیکی رمزگذاری شده ارسال کنید تا نحوه‌ی استفاده از نرم‌افزار را فراموش نکنید.

- جزئیات مربوط به نامه الکترونیکی از جمله عنوان و آدرس‌های پست الکترونیکی فرستنده و گیرنده‌ی پیام، رمزگذاری نمی‌شوند.

- GPG Suite برای سیستم‌های مک، GPG4win برای ویندوز و لینوکس، Thunderbird با افزونه‌ی مرورگر Enigmail و Mailvelope چند نمونه از نرم‌افزارهای رمزگذاری پست الکترونیکی هستند.

Committee to Protect Journalists

استفاده‌ی امن و مطمئن از اینترنت

روزنامه‌نگاران به اینترنت نیاز دارند اما لزوماً نمی‌خواهد رسانندگان خدمات اینترنتی، کافی‌نت‌ها یا هتل‌هایی که وای-فای رایگان دارند، از جزییات فعالیت‌شان در فضای مجازی مطلع شوند. خلافکاران و دشمنان خبره می توانند به سرقت اطلاعات روزنامه‌نگارانی که از سایت‌های ناامن و یا وای-فای عمومی استفاده می‌کنند، مبادرت ورزند یا آنان را هدف نظارت امنیتی قرار دهند.

برای استفاده امن از اینترنت:

- دقت کنید تمام آدرس‌های اینترنتی با https شروع شده و کنار آن آیکن قفل دیده شود، مانند (https://cpj.org). این نشان می‌دهد که ترافیک مبادله شده میان شما و تارنمای مورد نظر رمزگذاری شده است. با استفاده از افزونه‌ی مرورگر HTTPS Everywhere که توسط بنیاد مرزهای الکترونیکی طراحی شده، از امنیت تمام تارنماهایی که به آنها مراجعه می کنید، اطمینان یابید.
- مطمئن شوید که آدرس تارنما درست است و اسپوف (جعل) نشده باشد. به املای آدرس (url) دقت کنید و مطمئن شوید با https شروع شده باشد.
- با نصب ادبلاکر (ad-blocker) از خود در برابر بدافزارهای اینترنتی محافظت کنید. این بدافزارها اغلب ضمیمه تبلیغات بالاپر یا پاپ آپ هستند. استفاده از ادبلاکرها به شما امکان می‌دهد تا تارنماهای منتخب خود را از فیلترشدن مستثنی کنید.

- برای مسدود کردن تارنماها و تبلیغ‌کنندگانی که فعالیت فضای مجازی شما را رصد می‌کنند، افزونه‌ی Privacy Badger نصب کنید.

- هنگامی که از بلوتوث و سایر اپلیکیشن‌های اشتراک اطلاعات استفاده نمی‌کنید، آنها را غیرفعال کنید.

- برای محافظت از ترافیک اینترنت خود از VPN استفاده کنید، مخصوصاً زمان اتصال به وای-فای عمومی که اصلا امن نیست و شما را در معرض خطر هک شدن و نظارت امنیتی قرار می‌دهد.

- از رایانه‌های عمومی استفاده نکنید مخصوصا در کافی‌نت یا اتاق خبر. در صورتی که مجبور به استفاده از این نوع رایانه‌ها شدید، در انتهای کار از حساب‌های کاربری خود خارج شده و سابقه مرور خود را پاک کنید.

- با نصب مرورگر رایگان تور (Tor Browser Bundle) می‌توانید بطور ناشناس از اینترنت استفاده کنید. Tails یک سیستم عامل رایگان دیگر است که ترافیک اینترنت شما را به طور اجباری از شبکه‌ی تور عبور می‌دهد. این توصیه مخصوصاً متوجه روزنامه‌نگارانی است که درباره‌ی مطالب حساس تحقیق می‌کنند، مثلا فساد حکومتی در میان مسئولان عالی رتبه‌ی کشورهای دارای توانمندی تکنولوژیکی بالا.

عبور از مرزها:

بسیاری از روزنامه نگاران هنگام عبور از مرز، اطلاعات کاری و شخصی به همراه خود دارند و ممکن است نخواهند افراد دیگر به دستگاه‌هایشان دسترسی داشته باشند. وقتی ماموران مرزی دستگاهی را از دیدرس شما خارج می‌کنند، این فرصت را دارند که دستگاه شما را بگردند، به حساب‌های کاربری روی آن دسترسی یافته، اطلاعات روی آن را کپی کرده، و یا جاسوس‌افزار روی آن نصب کنند. به روزنامه‌نگارانی که قصد عبور از مرزهای ایالات متحده را دارند توصیه می‌شود به یادداشت ایمنی CPJ، "چیزی برای اظهارندارم" رجوع کنند.

قبل از سفر:

- دقت کنید چه اطلاعاتی روی دستگاه‌های شما ذخیره شده و آیا این اطلاعات می تواند آشنایانتان را در معرض خطر قرار دهد. فرض را بر این قرار دهید که همان بررسی موشکافانه‌ای که متوجه دفترچه‌های یادداشت و مطالب چاپی داخل چمدانتان می‌شود، متوجه دستگاه‌هایتان هم خواهد شد.

- از تمام دستگاه‌های خود در یک هارد خارجی یا حساب ابری نسخه‌ی پشتیبان تهیه کنید. اطلاعاتی که مایل نیستید ماموران مرزی به آن دست پیدا کنند را از روی دستگاه‌های خود پاک کنید.

- در صورت امکان، برای سفرتان دستگاه‌هایی خالی از هر نوع اطلاعات شخصی بخرید، به خصوص اگر در حال کار بر روی گزارشی حساس هستید. اگر قصد به همراه بردن یک دستگاه شخصی یا کاری را دارید، ابتدا از محتوای آن نسخه‌ی پشتیبان تهیه کرده و سپس دستگاه را کاملا پاک یا تنظیم مجدد کنید.

- گزینه‌ی رمزگذاری کامل دیسک را برای همه دستگاه‌های خود فعال کنید تا مطمئن شوید دسترسی به اطلاعات شما بدون گذرواژه ممکن نیست. درباره‌ی محدودیت‌های رمزگذاری در کشور مقصد تحقیق کنید تا مطمئن شوید بر خلاف قانون عمل نمی‌کنید. آگاه باشید که نیروهای امنیتی ممکن است به طور قانونی مجاز به درخواست گذرواژه‌ی شما باشند. اگر احتمال آن وجود دارد که در مرز متوقف شوید، قبل از سفر با کارفرما یا وکیل خود مشورت کنید.

- قبل از عبور از مرز و دسترسی به اتصال اینترنتی امن از تمام حساب‌های کاربری موجود در دستگاه‌های خود خارج شده و تمام اپلیکیشن‌ها را از روی آنها پاک کنید.

- سابقه مرورگر خود را در تمام دستگاه‌هایتان پاک کنید. (توجه: رساننده‌ی خدمات اینترنتی شما همچنان سابقه‌ی تارنماهایی که از آن بازدید کرده‌اید را در اختیار خواهد داشت.)

- به جای استفاده از داده‌های بیومتریک (زیست‌سنجشی) مانند صورت یا اثر انگشت، تمام دستگاه‌های خود را با رمز عبور یا گذرواژه قفل کنید.

- قابلیت پاک کردن از راه دور را در دستگاه‌های خود فعال کرده و با فرد قابل اعتمادی هماهنگ کنید تا در صورتی که بازداشت شدید دستگاه‌های شما را از راه دور پاک کند.

در پایانه‌ی مرزی:

- برای فعال کردن رمزگذاری دیسک، دستگاه‌های خود را خاموش کنید.

- هنگام عبور از بازرسی، حواستان به دستگاه‌هایتان باشد.

- تا زمانی که از فرودگاه دور نشده‌اید، گوشی خود را روشن نکنید. تمام تماس‌ها و پیام‌های کوتاه از طریق رساننده‌ی خدمات محلی هدایت می‌شوند که ممکن است این محتوا را جمع آوری کرده یا آن را با مقامات به اشتراک بگذارد. هنگام اتصال به وای-فای فرودگاه از VPN استفاده کنید.

- اگر دستگاهی در مرز ضبط شد یا چیزی به آن وصل شد، فرض را بر این قرار دهید که دستگاه مخدوش شده و تمام اطلاعات روی آن کپی شده است.