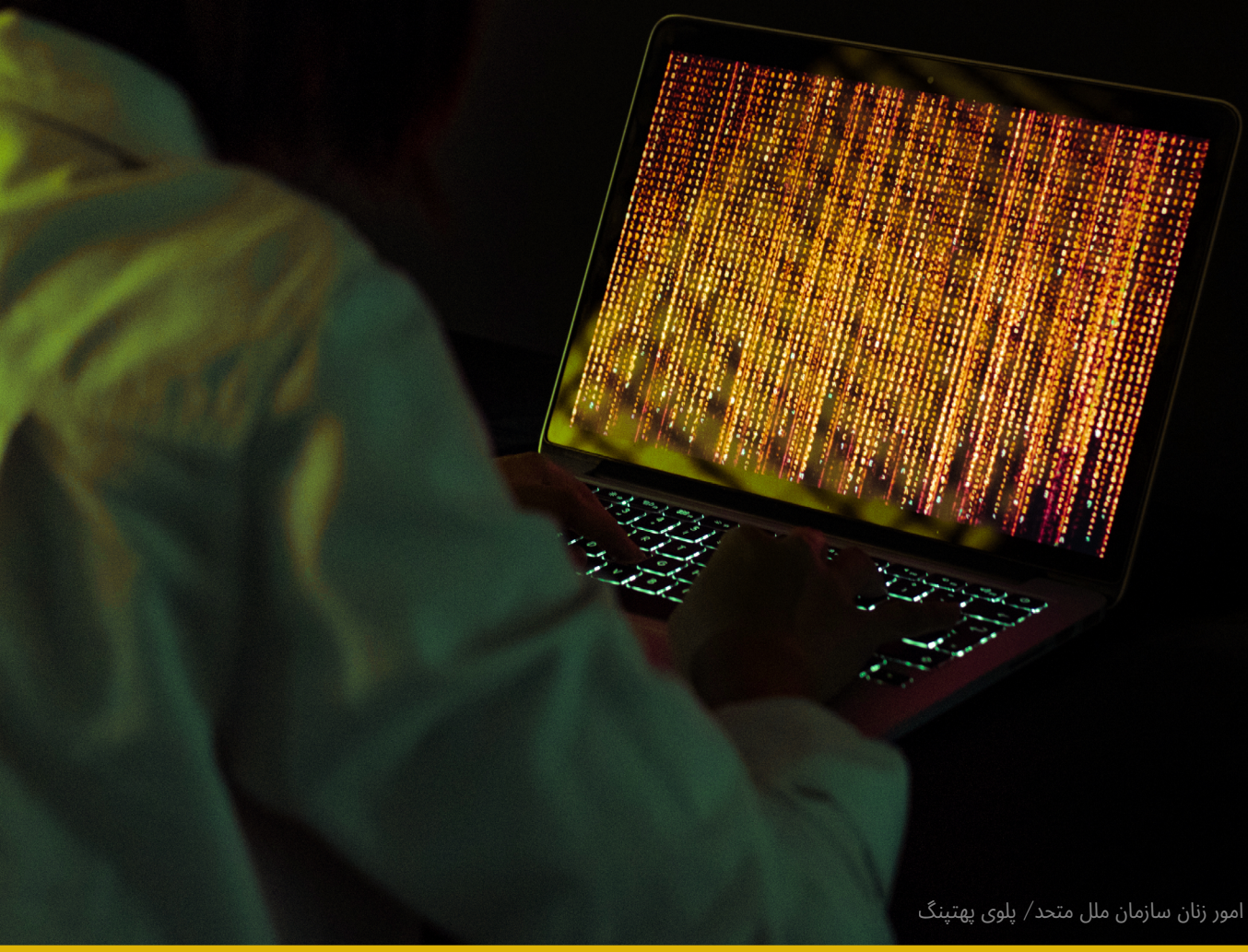
سند رهنمایی

محافظت آنلاین و امنیت دیجیتال:

رهنمود برای مدافعان حقوق بشر



تصویر: دفتر امور زنان سازمان ملل متحد/ پلوی پهتپنگ

UNAMA

UN WOMEN

فهرست مطالب

در مورد این سند

این سند منبع در اصل توسط هیئت معاونت سازمان ملل متحد برای عراق (UNAMI) تهیه شده است و هدف آن افزایش آگاهی و کاهش خطرات آنلاین مدافعان حقوق بشر، فعالان جامعه مدنی و کارکنان رسانه ها در فضای دیجیتال است که با آن مواجه هستند. متن اصلی بادرنظرداشت شرایط افغانستان توسط بخش حقوق بشر یوناما (یوناما) ودفتر ملل متحد برای زنان افغانستان ترتیب شده است.

رفع مسولیت

هیئت معاونت سازمان ملل متحد در افغانستان و دفتر ملل متحد برای زنان افغانستان از این فرصت برای ترویج فعالیت ها و نشرات خود با همکاری شرکا استقبال می کنند. لطفاً توجه داشته باشید که اطلاعات، نظریات و توصیه‌ها (شامل نرم‌افزارها و برنامه‌های کاربردی توصیه‌شده) توسط نویسندگان این رهنمود فقط برای اهداف اطلاعات عمومی ارائه شده است و لزوماً بیانگر دیدگاه یوناما/ دفتر ملل متحد برای زنان افغانستان (UNAMA/UN Women) نیست.

در حالی که نویسندگان این سند سعی در ارائه اطلاعات به روز و صحیح در زمان انتشار داشته اند، فناوری اطلاعات و تهدیدات امنیت دیجیتال به سرعت تغییر می کنند و بنابراین صحت آن را نمی توان برای همیشه تضمین کرد. به این ترتیب، یوناما/دفتر ملل متحد برای زنان هیچ گونه نمایندگی یا ضمانتی در مورد کامل بودن، سنخیت، قابل اطمینان بودن، مناسب بودن یا در دسترس بودن با توجه به اطلاعات، محصولات یا خدمات مندرج در اینجا، را ندارند.

کاربران باید صحت و امنیت فعلی اطلاعات یا نرم افزار را قبل از استفاده بررسی کنند. منابع در قسمت اخیر این رهنمود ارائه شده اند تا به کاربران کمک کند تا در مورد روش ها و نرم افزارهای مصون به روز بمانند.

۱. معرفی

امنیت دیجیتال و حقوق بشر در افغانستان

فناوری‌های دیجیتال می‌تواند فرصت‌های دادخواهی را برای، دفاع و اعمال حقوق بشر را مساعد سازند. این به طور فزاینده ای نحوه دسترسی افراد و به اشتراک گذاری اطلاعات را شکل می دهد و می تواند یک نشست برای بحث و مناظره باشد. این فرصت‌ها زمانی می‌توانند اهمیت ویژه‌ای پیدا کنند که حقوق و آزادی‌های اساسی در فضاهای فیزیکی یا «آفلاین» در معرض تهدید و محدود شدن قرار گیرد. با این حال، فناوری های دیجیتال می تواند برای سرکوب، محدود کردن و نقض حقوق بشر، به عنوان مثال از طریق نظارت و سانسور استفاده شوند. آنها همچنین می توانند توسط بازیگران دولتی و هم توسط شهروندان خصوصی برای تسهیل سوء استفاده و آزار و اذیت سیستماتیک موجود مورد استفاده قرار گیرند و اغلب باعث تقویت تبعیض و به حاشیه راندن می شوند.

از زمان تسلط طالبان بر افغانستان در ۱۵ آگست ۲۰۲۱، مشارکت زنان در زندگی روزمره و عمومی در نتیجه اقدامات مقامات برحال برای محدود کردن آزادی گشت و گذار زنان، دسترسی به کار و تحصیل و اعمال حقوق و آزادی های اساسی به طور قابل توجهی کاهش یافته است.[۱] موازی به آن، فضای مدنی و آزادی رسانه ها به میزان قابل توجهی کاهش یافته است.[۲] در این زمینه، فضای دیجیتال یک انتخاب مهم برای افغان‌ها، به‌ویژه زنان و دختران، فراهم کرده است تا نظریات و تجربیات خود را به اشتراک بگذارند، تجمع نمایند، در موضوعات مهم مشارکت کنند و برای حقوق خود دادخواهی کنند. با وجود این، فضاهای دیجیتال از خطرات و محدودیت‌هایی که در جاهای دیگر دیده می‌شود عاری نیست، طبق گزارش سخنان نفرت‌انگیز جنسیتی که زنان برجسته افغان را هدف قرار می‌دهد، از زمان تسلط طالبان سه برابر شده است[۳] و افرادی به دلیل ارسال محتوای آنلاین که انتقادی از مقامات برحال تلقی می شود، دستگیر شده اند.

خطرات امنیت دیجیتال برای زنان افغان

در نومبر ۲۰۲۳، بخش حقوق بشر هیئت معاونت ملل متحد در افغانستان (یوناما) و دفتر ملل متحد برای زنان در افغانستان رایزنی هایی با زنان در رسانه ها و جامعه مدنی برای درک بهتر دسترسی زنان افغان به فضای دیجیتال، از جمله خطرات و چالش های پیش روی زنان، و توصیه هایی برای اینکه چگونه می توان از حقوق و آزادی های خود در فضای دیجیتال محافظت کرد، را انجام دادند.

خطرات اصلی ذکر شده توسط زنان عبارت بودند از:

- نظارت و هک کردن حساب‌های رسانه‌های اجتماعی و پلت‌فرم‌های پیام‌رسان توسط اعضای مقامات حاکم و عموم مردم که منجر به تهدید و آزار و اذیت، چه آنلاین و چه آفلاین می‌شود.
- سوء استفاده جنسیتی آنلاین، اغلب به طور خاص زنان را به دلیل نمایه عمومی آنها که در رسانه ها یا جامعه مدنی کار می کنند، هدف قرار می دهد.

---

۱ برای کسب اطلاعات بیشتر، به گزارش های دفتر ملل متحد برای زنان، یوناما و IOM در مورد مشاوره با زنان افغان در داخل کشور که در نومبر ۲۰۲۳، جولای ۲۰۲۳، اپریل ۲۰۲۳، جنوری ۲۰۲۳ و آگست/سپتمبر ۲۰۲۲ انجام شده است، مراجعه کنید. وضعیت حقوق بشر در افغانستان: گزارش دفتر کمیساریای عالی حقوق بشر، ۱۱ سپتمبر ۲۰۲۳، A/HRC/٥٤/٢١.

۲ همکاری با سازمان ملل متحد، نمایندگان و سازوکارهای آن در زمینه حقوق بشر: گزارش سرمنشی، ۲۱ اگست ۲۰۲۳، Gehrig, M . A/HRC/٥٤/٦١. ۲۰۲۲. محدودیت های رسانه ای و پیامدهای آن بر برابری جنسیتی در افغانستان. کابل: دفتر ملل متحد برای زنان

۳ شاهد افغان. ۲۰۲۳. خشونت در پشت پرده: افزایش خشونت آنلاین، زنان افغان را ساکت می کند.

- doxing، که در آن اطلاعات شخصی مانند آدرس و شماره تلفن یافت می شود و به صورت عمومی به صورت آنلاین به اشتراک گذاشته می شود.
- جعل هویت در رسانه‌های اجتماعی، که در آن شخصی با استفاده از اطلاعات شناسایی شخصی که از یک فرد به سرقت رفته است، یک نمایه جعلی در رسانه‌های اجتماعی ایجاد می‌کند و به قصد بی‌اعتبار کردن آن‌ها، پست‌هایی را به نام آنها ارسال می‌کند.

زنان مجموعه ای از توصیه ها را در رابطه با اقداماتی که می توانند برای بهبود امنیت دیجیتال خود انجام دهند ارائه کردند. اینها عبارت بودند از:

- تدویر برنامه های آموزشی، نه تنها به منظور بهبود ظرفیت آنها برای محافظت از خود در برابر خطرات امنیتی دیجیتال، بلکه به طور کلی برای افزایش تسلط دیجیتالی و اعتماد به نفس آنها در استفاده از فناوری های دیجیتال.
- پشتیبانی و منابع اضافی به زبان‌های دری و پشتو، زنان خاطر نشان نمودند که بیشتر رسانه‌های اجتماعی و پلت‌فرم‌های پیام‌رسان (فیس‌بوک، اینستاگرام، ایکس، واتس‌اپ، سیگنال) منابع یا اطلاعاتی به این لسان ها ندارند.
- پشتیبانی مالی و فنی در مورد استفاده از نرم افزارها و برنامه های کاربردی با هدف بهبود امنیت دیجیتال، به عنوان مثال: خدمات به اشتراک گذاری و ذخیره سازی امن اسناد، تجزیه و تحلیل خطر امنیت دیجیتالی و VPN.

II. ده اصل برتر محافظت از کمپیوتر و تیلفون همراه

این بخش "ده نکته برتر" برای بهبود امنیت دیجیتال کاربران را ارئه می نماید. این مراحل اولیه در واقع یک نقطه ورود را به موضوعات اصلی که در فصول بعدی در مورد آن توضیحات مفصل ارائه خواهد گردید، فراهم می سازد.

نکته اول: سیستم عملیاتی، سخت افزار، اپلیکیشن ها، تیلفون و نرم افزار را به گونه منظم تجدید (update) نمایید.

شرکت ها سیستم های عملیاتی و اپلیکیشن های خویش را به گونه منظم تجدید (update) می نمایند، تا به خلا های امنیتی رسیدگی صورت گیرد. تجدید (update) منظم می تواند میزان محافظت کاربران را در برابر خلاهای های امنیتی به گونه قابل ملاحظه افزایش بخشد.

در ویندوز ۱۱، کاربران می توانند مشخص سازند که آخرین تجدید (update) را چه زمان و چگونه دریافت نمایند، تا دستگاه ها بتوانند به شکل منظم و مصون فعالیت کنند. جهت اینکه گزینه ها به شکل درست مدیریت شوند و تجدید (update) موجود مشاهده شود، لطفاً گزینه بررسی تجدید ویندوز (Check for Windows updates) را انتخاب نمایید. و یا اینکه گزینه **آغاز > تنظیمات > تجدید یا اپدیت ویندوز (Start > Settings > Windows Update)** را انتخاب نمایید.

- برای Mac، رهنمود های موجود را در اینجا دنبال نمایید.
- برای تجدید (update) تیلفون Android، رهنمود های موجود را در اینجا دنبال نمایید.
- برای تجدید (update) تیلفون iPhone (iOS) به ذخیره اپلیکیشن بروید (Go to the App Store) و رهنمود های موجود را در اینجا دنبال نمایید.

تجدید (update) منظم هرگونه سیستم های عملیاتی، اپلیکشین ها و نرم افزار های که مورد استفاده قرار می گیرد، باید در اولویت قرار داشته باشد.

نکته دوم: در تمام دستگاه ها رمز های نیرومند ایجاد نمایید

کاربران باید اطمینان حاصل نمایند که تمام رمز ها از ویژگی های ذیل برخوردار باشند:

- باید طولانی باشد (بیشتر از ۱۲ کرکتر باشد).
- باید مغلق باشد (ترکیبی از حروف بزرگ و کوچک، اعداد و سمبول ها باشد).
- باید تصادفی باشد، یعنی عاری از کلمات معمول و یا شخصی، تسلسل اعداد و غیره باشد.
- باید واحد و مشخص باشد (برای هر حساب یک رمز واحد و مشخص وجود داشته باشد).
- باید محرم باشد (نباید به آسانی روی یک کاغذ یا یک دستگاه دریافت شود).

لطفاً جهت دریافت معلومات مزید در مورد چگونگی ایجاد، مدیریت و ذخیره سازی محرمانه تمام رمز ها، به بخش III مراجعه نمایید.

نکته سوم: در صورت امکان از احراز هویت چند عاملی (MFA) استفاده به عمل آورید

- احراز هویت چند عاملی (MFA)، میزان امنیت دیجیتال را به گونه قابل ملاحظه افزایش می بخشد.
- پلیکیشن های که مختص برای احراز هویت چند عاملی (MFA) طراحی گردیده اند، مانند Duo Mobile، Aegis Authenticator و Google Authenticator، معمولاً در مقایسه با تصدیق پیام های کتبی (SMS) از امنیت بیشتر برخوردار اند.

لطفاً جهت دریافت معلومات مزید و لینک ها با اپلیکیشن های توصیه شده، به بخش III مراجعه نمایید.

نکته چهارم: نرم افزار شناسایی نقطه پایان و پاسخدهی (EDR) (ضد بدافزار) را نصب نمایید.

- نرم افزار های مخرب می توانند سبب تخریب یک دستگاه شوند، اطلاعات شخصی یا سرمایه های مالی را به سرقت ببرند و یا یک دستگاه را از راه دور کنترول نمایند.
- نرم افزار شناسایی نقطه پایان و پاسخدهی (EDR) از دستگاه مورد نظر در برابر بدافزار (malware) در انترنت محافظت می نماید.
- در هر یک از دستگاه های که از ویندوز، iOS، Linux، Mac و Android برخوردار می باشد، نسخه های مجاز نرم افزار شناسایی نقطه پایان و پاسخدهی (EDR) را نصب نمایید. هیچگاه از نرم افزار کرک شده "cracked software" استفاده نکنید.
- مهم است که نرم افزار رایگان را فقط از منابع قابل اعتماد دریافت کنید.
- اپلیکیشن های مانند Malwarebytes و Avira را نصب نمایید.

لطفاً جهت دریافت معلومات مزید، به بخش IV مراجعه نمایید.

نکته پنجم: از یک مرورگر (browser) مصون استفاده نمایید

- مرورگر (browser) در حقیقت به مثابه ویندوز انترنت عمل می نماید. هرگاه ویندوز از مصونیت لازم برخوردار نباشد، دسترسی و جهت یابی (navigation) مصون نیست و می تواند یک بستر مناسب برای ملوث شدن توسط افزار های مخرب باشد.
- بسیاری از مرورگر ها (browser) ابزار های تجارتی بوده که به منظور جمع آوری اطلاعات، ردیابی و هدف گیری دیتا به هدف بازاریابی مورد استفاده قرار می گیرند.
- از مرورگرهای (browser) مصون مانند Ghostery Dawn، Firefox Focus، Brave، Firefox و DuckDuckGo استفاده به عمل آورید. نرم افزار مرورگر (browser) را به گونه منظم تجدید (update) نمایید.
- امنیت گزینه های افزونه (add-ons/extensions) را قبل از آنکه در مرورگر (browser) علاوه شوند، بررسی نمایید.

لطفاً جهت دریافت معلومات مزید به بخش V در ذیل مراجعه نمایید.

نکته ششم: یک شبکه خصوصی مجازی (VPN) را نصب نمایید

- VPN مخفف "شبکه خصوصی مجازی" می باشد، یعنی به خدماتی اطلاق می گردد که به صورت آنلاین از طریق ایجاد یک تونل رمزگذاری شده برای دیتای کاربران و پنهان کردن IP آدرس IP address کاربران، از اتصال انترنتی و محرمیت کاربران محافظت می نماید. این گزینه زمنیه را برای استفاده مصون از Wi-Fi عامه فراهم می سازد. بدون استفاده از گزینه محافظتی شبکه خصوصی مجازی (VPN)، امکان دارد دستگاه ها و موقعیت های آنها ردیابی شوند و یا دیتا رهگیری شود.
- شبکه خصوصی مجازی (VPN) را با دقت کامل انتخاب نمایید. خدمات رایگان و غیررایگان وجود دارند که حاوی نرم افزار های مخرب می باشند و اطلاعات کاربران را به شخص ثالث به فروش می رسانند و یا به خاطر در اختیار قرار دادن اطلاعات مرتبط به کاربران با دولت ها همکاری می نمایند.
- شبکه های خصوصی مجازی (VPNs) که معمولاً در زمان نشر مصون پنداشته می شوند، عبارت از شبکه های خصوصی مجازی TunnalBear، Psiphon و Riseup می باشند.

لطفاً جهت دریافت معلومات مزید به بخش III در ذیل مراجعه نمایید.

نکته هفتم: از نرم افزار ها و اپلیکیشن های مصون منبع باز (open-source) استفاده

- به صورت عموم نرم افزار ها و اپلیکیشن های منبع باز (Open-source) در مقایسه با برنامه های اختصاصی مصون تر می باشند، زیرا آنها کد منبع خود را به کاربران ارائه می نمایند. سپس، این کد منبع به شکل دوامدار تجدید (update) می شود، تا به آسیب پذیری های امنیتی رسیدگی لازم صورت گیرد.
- استفاده از نرم افزار ها و اپلیکیشن های منبع باز (open-source)، به کاربران اجازه نمی دهد تا از نرم افزار های اختصاصی غیرقانونی یا کرک شده "cracked" بدون مجوز، استفاده نمایند. برنامه های غیرقانونی یا کرک شده "cracked" می توانند حاوی عناصر مخرب باشند، که دستگاه ها را صدمه می زنند و هیچگاه نباید از آنها استفاده صورت گیرد.
- به خاطر باید داشت که تمام اپلیکیشن های منبع باز (open-source) مصون نمی باشند: بناءً، همواره باید قبل از نصب کردن یک نرم افزار یا اپلیکیشن جدید، توصیه های کارشناسان امنیت دیجیتال مدنظر گرفته شود. بهتر است از برنامه‌هایی استفاده کنید که سابقه استفاده قوی دارند و برنامه‌ها و خطمشی‌های امنیتی را در مورد مسائل و حریم خصوصی به وضوح می شناسند.

نکته هشتم: برنامه ها و نرم افزار ها را صرف از ذخیره‌گاه های اپلیکیشن (App Stores) شناخته شده دانلود نمایید

- ذخیره‌گاه های اپلیکیشن (App Stores) ناشناخته حاوی ده ها اپلیکیشن و برنامه های ملوث با نرم افزار های مخرب و در های عقبی (back doors) می باشند، که به مرجع تولید کننده اجازه می دهد تا دستگاه ها را مدیریت و کنترول نماید.
- برای دانلود، صرف از ذخیره‌گاه های اپلیکیشن (App Stores) شناخته شده و ویب سایت های رسمی اپلیکیشن استفاده به عمل آورید: Amazon Appstore، Google Play و Apple App Store.

نکته نهم: کمپیوتر ها و تیلفون ها را رمزگذاری نمایید

- رمزگذاری زمینه را برای حفظ محرمیت فراهم ساخته و برای امنیت اطلاعات ضروری می باشد.
- از رمزگذاری استفاده به عمل آورید، تا پیام های رمزگذاری شده را ارسال نمایید، اطلاعات را به گونه مصون ذخیره نمایید، انترنت را به صورت ناشناس بررسی (browse) نمایید و اطلاعات را با مصونیت بیشتر در میان بگذارید.

لطفاً جهت دریافت معلومات مزید در مورد ابزار های رمزگذاری به بخش VI مراجعه نمایید.

نکته دهم: نسخه پشتیبان (Backup) دیتای خود را تهیه نمایید

- پروسه پشتیبان (Backup) به مثابه اینست که شما اطلاعات ارزشمند خود را در یک سیف ذخیره می کنید، تا در صورت مفقود شدن، صدمه دیدن و یا هک شدن دیتای اصلی، آنها را بازیابی نموده بتوانید.
- ابزار پشتیبان (Backup) ارائه شده در سیستم عملیاتی (در ویندوز یا MacOS) را طور غیر خودکار (manual) و از تکمیل باقاعده پشتیبانی (Backup) اطمینان حاصل نمایید.
- نسخه های پشتیبان (Backup) دیتا را برای ذخیره سازی رمزگذاری نمایید.
- نسخه پشتیبان (Backup) را در یک هارد دیسک خارجی و یا خدمات ابری (cloud-based service)، مانند Google Drive ذخیره نمایید.

لطفاً جهت دریافت معلومات مزید به بخش VI مراجعه نمایید.

نکته تکمیلی: حالت قفل کردن اضطراری

- استفاده کننده گان آی فون در صورت حملات پیچیده و هدفمند سایبری به گزینه قفل کردن اضطراری Lockdown Mode به منظور مصونیت دسترسی دارند.
- حالت قفل اضطراری عملکرد برنامه های مشخص مانند اپلیکشن ها، ویب سایت ها، و نمایه ها را محدود می نماید تا احتمال نفوذ سپای ویر را به دیتای ذخیره شده در وسیله را کم نماید.

III. رمز های قوی را ایجاد نمایید و گزینه احراز هویت چندعاملی (MFA) را فعال سازید

رمز های قوی

رمز های قوی تهداب و بنیاد حفاظت دیجیتال را تشکیل می دهد. نیروی این رمز ها سبب می شود تا در برابر حملات بیشمار که رمز ها را مورد هدف قرار می دهند، مانند عملیات فیشنگ (phishing)، keyloggers و سایر حملاتی که هدف آن رهگیری دیتا و یا ورود غیرمجاز به حساب ها یا دیتای محافظت شده می باشد، مقاومت نمایند.[٤]

برای دفاع موثر در برابر این حملات، باید از طریق ایجاد رمز های نیرومند و تغییر دادن منظم آنها از ورود آنها جلوگیری نمود.

یک رمز نیرومند عمدتاً از ویژگی های ذیل برخوردار می باشد:

١. طولانی

از یک رمزی که بیشتر از ١١ کرکتر داشته باشد، استفاده نمایید. به هر اندازه که رمز کوتاهتر باشد، به همان اندازه می تواند سریعتر شناسایی شود.

٢. مغلق

از یک رمزی که از حروف بزرگ و کوچک، اعداد و سمبول ها ترکیب یافته باشد، استفاده نمایید.

٣. تصادفی

از استفاده از اعداد و کلمات دارای تسلسل و یا استفاده از معلومات شخصی و خانوادگی جداً خودداری نمایید. از کاربرد تاریخ های تولد، اسم های اعضای خانواده و اسیم های حیوانات خانگی در رمز اجتناب ورزید.

٤. حفظ نمودن آسان

به فراموشی سپردن رمز ها در واقع چرخه بازیابی را که به اطلاعات بیشتر نیاز دارد، به حرکت می آورد. هرگاه به خاطر سپردن همزمان چند رمز دشوار باشد، در آن صورت از گزینه مدیریت کننده رمز (password manager) (در قسمت ذیل) استفاده نمایید.

٥. محرم

رمز ها را ایجاد و ذخیره نمایید، اما صرف در موقعیت های مصون نه در موقعیت های غیرمصون. موقعیت های غیرمصون عبارت از یادداشت نمودن مستقیم در مرورگر (browser)، اپلیکیشن یادداشت های تیلفون، اپلیکیشن یادآوری تیلفون، یادداشت های کاغذی چسپ دار روی کمپیوتر و یا یادداشت در یک کتابچه/اجندا، می باشند. این موقعیت ها غیرمصون هستند، چون دسترسی به آنها سهل است.

٤ حملاتی که به منظور افشا ساختن رمز ها انجام می یابند عبارت از حملات موسوم به مردی در وسط (man-in-the-middle) یا (MITM)، حملات قوای بیرحم (brute force)، حملات فرهنگ لغات (dictionary attacks) و حملات مبتنی بر اعتبار (credential stuffing) می باشد. لطفاً برای دریافت معلومات مزید در مورد حملات مروج رمز، به (Password Cracking 101: Attacks & Defenses Explained.)مراجعه نمایید.

٦. واحد و مشخص

هر حساب یا خدمات باید یک رمز واحد و مشخص خود را داشته باشد. شناسایی رمز یکی از حساب ها در حقیقت منتج به آسیب پذیری سایر حساب های که از عین رمز استفاده می کنند، خواهد شد.

۷. تغییر دادن منظم

مدت زمانی که قرار است قبل از تغییر دادن رمز از آن استفاده شود در حقیقت به میزان خطراتی که کاربران با آن روبرو اند، بستگی دارد. در شرایط عادی توصیه می شود که باید در هر ربع سال یکبار رمز تغییر یابد. حین تغییر دادن رمز، لازم است تا کاربراین به صورت مکمل از اپلیکیشن و یا خدمات موجود در تمام دستگاه ها خارج شوند.

۸. اصلی

از نمونه های معمولی کیبورد مانند "Qwerty۱۲۳٤٥" یا "Password۱۲۳" استفاده نکنید.

رمز ها را می توان در حافظه های پنهان (caches) یا مدیریت کننده های رمز (password managers) که دسترسی به آن دشوار می باشد، ذخیره (save) نمود. این حافظه های پنهان (caches) در واقع ایجاد کننده رمز های نیرومند هستند و می توان تعداد زیاد رمز ها را در آن ذخیره (save) نمود.

انواع مدیریت کننده های رمز (password managers) که در زمان نشر مصون پنداشته می شوند، قرار ذیل اند:

۱. KeePassXC
۲. Bitwarden

احراز هویت چندعاملی (MFA)

فعال ساختن ویژگی احراز هویت چندعاملی (MFA) زمینه را برای محافظت جدی در برابر هک شدن و فیشنگ (phishing) فراهم می سازد. احراز هویت چندعاملی (MFA) در حقیقت یک ویژگی اضافی بوده که از کاربران می خواهد یک کد رمز قابل استفاده واحد (single-use password) را وارد نمایند، که پس از وارد کردن رمز عادی ایجاد می شود. این رمز قابل استفاده واحد از طریق پیام کتبی (SMS) یا ایمیل به کاربر فرستاده می شود و یا از طریق یک اپلیکیشن ویژه تصدیق قابل دسترس می باشد.

بهترین روش برای فعال ساختن تصدیق دو مرحله یی، عبارت از فعال نمودن آن با استفاده از یک اپلیکیشن خارجی می باشد. اپلیکیشن های ذیل در زمان نشر، مصون پنداشته شده اند:

۱. Duo Mobile
۲. Aegis Authenticator (صرف برای Android)
۳. Google Authenticator (iOS یا Android)

IV. بدافزار (malware) را از بین ببرید

بدافزار (malware) چیست؟

نرم افزار مخرب یا بدافزار (malware) عبارت از اصطلاحی می باشد که عمدتاً برای یک نرم افزاری اطلاق می شود که به منظور آسیب رسانیدن، سوء استفاده و یا غیرفعال ساختن دستگاه ها، سیستم های عملیاتی و یا شبکه ها طراحی شده باشد. از اینگونه نرم افزار ها در سرقت دیتا، دسترسی غیرمجاز، غیرفعال ساختن یکعده یا تمام عملکرد ها (functions) و صدمه رسانیدن به دستگاه ها و یا هر شبکه مرتبط به آن، استفاده به عمل می آید.

"وایرس ها" صرف اعضای کوچک خانواده نرم افزار های مخرب می باشند، حالانکه انواع دیگر بدافزارهای (malware) مضرتر نیز وجود دارند که می توانند حین استفاده از انترنت به دستگاه ها نفوذ نمایند و آنها را ملوث سازند.

پروسه از بین بردن بدافزار (malware) مستلزم روی دست گرفتن اقدامات وقایوی دوامدار می باشد. ایجاد موانع در برابر ملوث شدن و نفوذ نرم افزار های مخرب، در واقع کاربران را یاری می رساند تا قبل از وارد شدن به دستگاه های شان، تهدیدات را از میان بردارند.

انواع مختلف نرم افزار های مخرب وجود دارند، مانند: Trojans، worms، ransomware، adware، spyware و غیره.

چگونه می توان از دستگاه ها در برابر بدافزار (malware) محافظت نمود؟

جهت محافظت از دستگاه ها در برابر بدافزار (malware) باید مراحل ذیل دنبال شوند:

۱. نرم افزار معتبر شناسایی نقطه پایان و پاسخدهی (EDR) را در هر دستگاه حاوی سیستم های ویندوز، Mac، Linux، iOS یا Android، به شمول تمام کمپیوتر ها و تیلفون های همراه، نصب نمایید. به خاطر باید داشت که صرف یک برنامه شناسایی نقطه پایان و پاسخدهی (EDR) باید نصب شود.

۲. برنامه ها و اپلیکیشن ها را صرف از ویب سایت های رسمی مربوطه دانلود نمایید.

۳. سیستم های عملیاتی و اپلیکیشن های هر دستگاه را به گونه منظم تجدید (update) نمایید.

٤. از شبکه های عامه و/یا غیرمصون Wi-Fi، بدون محافظت مناسب (مانند شبکه خصوصی مجازی "VPN") استفاده نکنید.

٥. هیچگاه بالای لینک های ارسال شده توسط اشخاص بیگانه و یا ایمیل ها یا پیام های مشکوک که حتی از جانب مخاطبین شناخته شده نیز دریافت شده باشند، کلیک نکنید.

٦. از در میان گذاشتن اطلاعات شخصی اجتناب ورزید.

۷. حین جستجوی انترنت، از یک بروسر (browser) مصون استفاده نمایید.

۸. برای مرورگر (browser) مورد نظر، افزونه های (add-ons) توصیه شده را نصب نمایید.

دو برنامه شناسایی نقطه پایان و پاسخدهی (EDR) که در زمان نشر، مصون پنداشته شده اند (نسخه رایگان و غیررایگان)، عبارت از Malwarebytes و Avira می باشند. توجه داشته باشید که نرم‌افزار ضد ویروس رایگان محافظت اولیه در برابر ویروس‌های عادی را ارائه می نماید در حالی که نرم‌افزار ضد ویروس خریداری شده محافظت پیشرفته‌تری را پیش کش می کند.

۷. انترنت را به گونه مصون جستجو نمایید

کاربران زمانی با حجم بلند خطرات روبرو می شوند که کمپیوتر یا تیلفون همراه شان با انترنت وصل می شود و آنان شروع به جستجو در انترنت و یا تامین ارتباط با دیگران می کنند.

به منظور بلند بردن میزان مصونیت خویش، از ابزار های مصون دسترسی به انترنت استفاده به عمل آورید. این امر مانع نظارت ارائه کنندگان خدمات، مراجع و یا هکر ها از فعالیت کاربران می شود.

روتر (router) تان را مصون نمائید

مرحله اول عبارت از مصون ساختن هاتسپات Wi-Fi در منزل یا محل کار می باشد، که عمدتاً از طریق تغییر دادن تنظیمات روتر (router) صورت می گیرد. اگر با مراحل مذکور آشنایی ندارید، لطفاً کمک تخنیکی مطالبه نمایید. برای اطلاعات اولیه در مورد نحوه تنظیم نمودن روتر، لطفاً به Security in a Box، «محافظت در برابر بدافزار: روتر خود را ایمن کنید»، که در اینجا قابل دسترس است مراجعه کنید: https://securityinabox.org/en/phones-and-computers/malware/.

۱. اسم کاربر (username) و رمز حساب مدیریت کننده روتر (router) را تغییر دهید.

۲. آدرس IP روتر (router) را تغییر دهید.

۳. از یک رمز قوی و خصوصی برای Wi-Fi استفاده نمایید.

٤. تنظیمات رمزگذاری را تنظیم نموده و گزینه WPA2-PSK (AES) را انتخاب نمایید.

٥. سیستم عملیاتی روتر (router) را تجدید (update) نمایید.

٦. اسم شبکه Wi-Fi را پنهان (hide) نمایید.

استفاده از هاتسپات های Wi-Fi عامه

شبکه های Wi-Fi عامه (در کافه ها، فروشگاه ها، مراکز خریداری، هوتل ها، میدان های هوایی، ترانسپورت عامه، رستورانت ها و غیره) معمولاً از لحاظ امنیتی ضعیف بوده و می توانند کاربران را با تهدیدات جدی روبرو سازند، منجمله:

۱. **تهدید کشف بسته (Threat of packet discovery)** مهاجمان (هکر ها) دیتا ارسالی یا دریافتی رمزگذاری ناشده را که از طریق شبکه های محافظت ناشده فرستاده شده باشند، نظارت نموده و آن را رهگیری می کنند.

۲. **حملات مردی در وسط (Man-in-the-Middle)** مهاجمان در هاتسپات ضعیف Wi-Fi نفوذ می نمایند، تا بخشی از ارتباط بین قربانی مورد هدف و هاتسپات باشند و بتوانند در مقابل دیتای در حال انتقال سد ایجاد کنند و در بسا موارد آنرا تغییر دهند.

۳. **شبکه های فریبنده Wi-Fi** مهاجمان برای اتصال عامه یک هاتسپات رایگان و باز را ایجاد و راه اندازی می نمایند و از آن به عنوان یک دهلیز جمع آوری دیتای کاربران استفاده می کنند.

هنگام استفاده از Wi-Fi عامه از خود محافظت نمایید

در صورت امکان به جای استفاده از وای فای عامه از اتصال سیار یا موبایل استفاده نمائید. به منظور محافظت از اطلاعات شخصی تان در برابر مهاجمان حین استفاده از نقاط ارتباطات عامه، رهنمود های ذیل را دنبال نمایید:

- تا حد امکان از استفاده از هاتسپات های ناشناخته/غیرمصون و یا انترنت عامه اجتناب ورزید.
- هرگاه شما از یک شبکه عامه استفاده می نمایید، اطمینان حاصل نمایید که قبل از استفاده از آن، برای تمام حساب ها احراز هویت چندعاملی (MFA) را فعال سازید.
- از فایروال (firewall) استفاده نمایید. شماری زیادی از سیستم های عملیاتی از این خدمات برنامه های ضد بدافزار (anti-malware)/ شناسایی نقطه پایان و پاسخدهی (EDR)، برخوردار می باشند. اپلیکیشن های که در زمان استفاده مصون پنداشته شده اند، قرار ذیل اند:

  GlassWire Comodo Avira

- در ویندوز، Microsoft Defender Firewall را راه اندازی کنید. دستورالعمل ها در اینجا قابل دسترس اند.
- از خدمات شبکه خصوصی مجازی (VPN) برای رمزگذاری اتصال انترنت و خصوصی نگهداشتن فعالیت آنلاین در هر شبکه استفاده به عمل آورید . شبکه های خصوصی مجازی (VPNs) که در زمان نشر مصون پنداشته شده اند، قرار ذیل اند:

  Riseup TunnelBear Psiphon ProtonVPN Windscribe

مرور گرهای مصون را استفاده کنید

بروسر (browser) ها دریچه اصلی دسترسی به انترنت به شمار می روند، بناءً در امنیت آنلاین نقش قابل ملاحظه ایفا می نمایند. بسیار ضرور است که یک مرورگر (browser) مصون به عنوان یک عنصر محافظت کننده در برابر سرقت و یا نقض محرمیت دیتا، انتخاب شود.

مرورگرهای (browser) که در زمان نشر مصون پنداشته شده اند، قرار ذیل اند:

Firefox Brave Ghostery Dawn DuckDuck Go Firefox Focus (برای تیلفون های iPhone)

لطفاً برای دریافت معلومات مزید در مورد مزایا و نواقص مرورگر های گوناگون، به رهنمودی که توسط بنیاد آزادی مطبوعات به نشر رسیده است و در اینجا قابل دسترس می باشد، مراجعه نمایید.

از انجن های جستجوی مصون استفاده نمائید

همچنان، باید با استفاده از انجن های جستجوی مصون که متضمن حفظ محرمیت می باشند، جستجو ها انجام یابند. بسیاری از انجن های جستجوی مروج، به شمول Amazon، Bing، Google، و Yandex ستندرد های حفظ محرمیت را تکمیل نمی کنند.

انجن های جستجوی کسه در زمان نشر بیشتر مصون و دارای حفظ محرمیت پنداشته شده اند، قرار ذیل اند:

DuckDuck Go Qwant StartPage

از افزونه های (extensions/add-ons) مرورگر مصون استفاده نمایید

افزونه های (extensions/add-ons) مرورگر، فعالیت یک برنامه را در برنامه دیگر مثل مرورگر (browser)، توسعه می بخشد. گزینه علاوه کردن (add-ons) در حقیقت نسخه کامل نرم افزار نبوده، بلکه بخش های از کدی می باشند که یک اتصال مشخص را تغییر می دهد. معمولترین گزینه علاوه کردن (add-ons) برای مرورگرها (browser) عبارت از تولبارهای (toolbar) می باشند که میانبر های (shortcut) فوری خدمات آنلاین را در اختیار کاربران قرار می دهند.

افزونه های (extensions/add-ons) مرورگر که باید دانلود شوند، آنهایی اند که میزان امنیت و حفظ محرمیت کاربران را افزایش می بخشند.

افزونه های ذیل در زمان نشر، برای کاربران زمینه امنیت بیشتر را فراهم می سازند:

Cookie AutoDelete Malwarebytes Ghostery Virus Total HTTPS Everywhere

Privacy Badger NoScript

VI. همه چیز در مورد رمزگذاری (encryption)

رمزگذاری (encryption) چیست؟

رمزگذاری (encryption) در اصطلاح عبارت از پروسه تبدیل نمودن دیتا از یک فارمت خوانا به یک کد مخفی می باشد، که تنها کاربرانی که "کلید" یا رمز مخفی را در اختیار دارند، می توانند آنرا "باز" نمایند.

رمزگذاری (encryption) دارای مزایای ششگانه ذیل می باشد

- زمینه را برای انسجام (یکپارچه سازی) و حفظ محرمیت دیتا فراهم می سازد.
- نهاد ها را کمک می نماید تا قواعد حفظ محرمیت و امنیت را رعایت نمایند.
- حین انتقال دیتا در دستگاه ها، از آنها محافظت می نماید.
- نهاد ها را کمک می نماید تا دفاتر شان را مصونیت بخشند.
- از مالکیت معنوی محافظت به عمل می آورد.
- حین انتقال دیتا در فضای ذخیره سازی ابری (cloud storage)، از آنها محافظت می نماید.

از رمزگذاری (encryption) می توان به منظور انجام دادن فعالیت های ذیل استفاده نمود

۱. ذخیره نمودن تصاویر، ویدیو ها و دیتا را در دستگاه ها به گونه مصون.
۲. در میان گذاشتن فایل ها و اسناد را به گونه مصون.
۳. ایمیل های خصوصی را به گونه مصون ارسال نمود.
٤. ذخیره سازی فایل ها را با استفاده از سرویس های ابری (cloud services) به گونه مصون.
٥. ارتباطات از طریق پیام ها یا تیلفون به گونه مصون.

الف. ارتباط مصون برقرار نمایید

"ارتباطات مصون" چیست؟

ارتباطات مصون عبارت از پروسه رمزگذاری ارتباطات کاربران با استفاده از یک یا چند پروتوکول امنیتی می باشد، تا اطمینان حاصل شود که تبادله دیتا میان فرستنده و گیرنده بدون دسترسی شخص ثالث جریان دارد. رمزگذاری

(Encryption) معمولاً یک متن ساده را به یک نوع کد مخفی مبدل می سازد که دیگران قادر به خواندن آن نیستند، حتی اگر قبل از مواصلت به گیرندگان مورد نظر، رهگیری شود. زمانیکه گیرندگان پیام را دریافت می کنند، دستگاه مربوطه آنها از کلید مشخص خود استفاد نموده تا اطلاعات را به یک متن ساده و خوانا مبدل سازد.

هرگاه یک اتصال رمزگذاری (Encryption) نشده باشد، در آن صورت دولت ها، گروه ها و افراد دارای پیشینه تخنیکی می توانند به ارتباطات گوش دهند و یا آنها را بخوانند و به محتویات آن دسترسی داشته باشند، رهگیری کنند و در آن تغییرات وارد نمایند، در آن بدافزار (malware) نصب کنند و بالاخره در درون سیستم در های عقبی (backdoors) را برای انتقال دیتا به دستگاه و از دستگاه باز نمایند.

ستندرد های امنیتی

معیارات ذیل برای انتخاب برنامه ها و اپلیکیشن های ارتباطات توصیه می شود، تا اطمینان حاصل شود که ارتباطات در برابر شنود، جاسوسی و دسترسی غیرمجاز به اطلاعات شخصی مصون می باشد.

- **ارتباطات** بین فرستنده و گیرنده باید با استفاده از گزینه انتها - به - انتها End-to-end (E2EE) رمزگذاری شود، تا حتی شرکت یا ارائه کننده خدمات نتواند به محتویات پیام ها دسترسی داشته باشند. پیام ها توسط فرستنده به صورت رمزگذاری شده (encrypted) صادر می شوند و تا زمانیکه به دستگاه گیرنده مواصلت نکند، رمزگشایی (decrypted) نمی شوند.

- **عدم ردیابی**، بدین معنا که شرکتی که اپلیکیشن مورد نظر را تولید نموده است، اطلاعات را ردیابی نمی کند و یا دیتای کاربران را جمع آوری نمی کند. شماری زیادی از شرکت های تجارتی راجع به کاربران اطلاعات جمع‌آوری نموده و آنرا به شرکت ها یا کشور های دیگر، مانند شرکت های تبلیغاتی و بازاریابی، به فروش می رسانند.

- طوری که در فوق تذکر داده شد، اپلیکیشن یا برنامه باید **منبع باز (open source)** باشد. نرم افزار منبع باز (open source) کد اپلیکیشن ها و برنامه ها را به منظور ارزیابی و تشخیص نقاط ضعف به متخصصین ارائه می نماید. همچنان، کد منبع باز (open source) زمینه را برای بررسی اینکه آیا شرکت تولید کننده اطلاعات و دیتای کاربران را جمع آوری می کند یا خیر، فراهم می سازد. بهتر است از برنامه‌هایی استفاده کنید که سابقه استفاده قوی دارند و برنامه‌ها و خط‌مشی‌های امنیتی را در مورد مسائل و حریم خصوصی به وضوح می شناسند.

- **باید یک گزینه ناشناس بودن قابل دسترس باشد**، بدین معنا که برنامه یا اپلیکیشن می تواند اطلاعات شخصی کاربران (اسم، شماره تماس، ایمیل آدرس، موقعیت جغرافیایی و ID دستگاه) را حتی در زمان ارسال و دریافت پیام ها، تماس های صوتی و ارسال و دریافت ضمایم (به شمول mp3، jpeg، pdf، doc و غیره) مخفی نگهدارد.

شماری زیادی از کاربران در مورد این نگران اند که آیا اپلیکیشن های مروج مانند فیسبوک مسنجر، وایبر، تلگرام، واتس اپ و غیره، معیارات فوق‌الذکر را تکمیل نموده اند یا خیر. بررسی گزارشات منظم شرکت ها در مورد شفافیت و ارزیابی های متخصصین امنیتی نشان دهندۀ آنست که اپلیکیشن های مذکور برخی از ستندرد های فوق را رعایت نموده، اما متأسفانه اکثراً آنها تمام معیارات را تکمیل نمی کنند.

توصیه ها برای اپلیکیشن های ارتباطات مصون

Signal مدیریت کننده خصوصی سیگنال (Signal Private Messenger) به صورت عموم به عنوان یکی از مصونترین اپلیکیشن های حفظ محرمیت مدنظر گرفته می شود و تمام معیارات فوق‌الذکر را به استثنای حفظ ناشناس بودن رعایت می کنند. برای اینکه سیگنال فعال شود، به یک شماره تیلفون نیاز است. اما، سیگنال اطلاعات را ردیابی نکرده و اطلاعات کاربران را جمع آوری نمی کند.

Wire این نرم افزار ستندرد های فوق‌الذکر را با یک اتصال سهل تکمیل می نماید. برای تیلفون همراه و کمپیوتر قابل دسترس می باشد. نیاز نیست که به عنوان یک برنامه یا اپلیکیشن نصب شود - می توان از آن به عنوان یک افزونه (extension) در مرورگر (browser) استفاده نمود.

Jitsi پلاتفورمJITSI MEET تامین کننده ارتباطات یا برگزاری جلسات آنلاین می باشد. یکی از مزایای عمده آن نسبت به سایر اپلیکیشن های که برای برگزاری جلسات مبتنی بر انترنت مورد استفاده قرار می گیرند، اینست که باعث ایجاد یک کانال رمزگذاری شده برای ارتباطات شده و ناشناس بودن را حفظ می نماید. حین استفاده از این پلاتفورم اصلاً برای ایجاد حساب کاربری یا وارد نمودن اطلاعات شخصی نیازی وجود ندارد. کاربران می توانند از طریق یک مرورگر (browser) از ویب سایت بازدید نمایند، یک چت باز کنند و لینک ها را با هر کسی که می خواهند به گفتمان دعوت نمایند، در میان بگذارند. اپلیکیشن Jitsi را می توان در کمپیوتر ها و تیلفون های همراه نصب نمود.

Tresorit این خدمات نیز اطلاعات را از انتها - به -انتها رمزگذاری می نماید. این نیز یک اتصال ساده بوده و طرز استفاده آن آسان می باشد و امنیت اطلاعات را حفظ می نماید و حین انتقال آنها را رمزگذاری می کند.

چگونه می توان ایمیل های مصون و رمزگذاری شده (encrypted) را با PGP ارسال نمود؟

بهترین روش برای حصول اطمینان از مصون بودن ایمیل ها، عبارت از رمزگذاری آنها با "PGP" می باشد. PGP مخفف "Pretty Good Privacy" (محرمیت بسیار خوب) می باشد. این یک سیستم رمزگذاری (encryption) است که هم به منظور ارسال ایمیل های رمزگذاری شده (encrypted) و هم به منظور رمزگذاری فایل های حساس از آن استفاده به عمل می آید. PGP ایمیل ها و ضمایم آنرا رمزگذاری می نماید، تا از طریق ایجاد یک جوره کلید خصوصی و عامه مورد نیاز برای "باز نمودن" اطلاعات، محرمیت ارتباطات را افزایش بخشد.

اطلاعات بیشتر در مورد رمزگذاری ایمیل ها در اینجا قابل دسترس است.

یادداشت:

PGP تنها زمانی قابل استفاده می باشد که فرستنده و گیرنده هر دو از اپلیکیشن ها یا برنامه های مدنظر گرفته شده برای رمزگذاری (encrypting) و رمزگشایی (decrypting) پیام ها، استفاده نمایند. تعداد بیشماری از برنامه ها و اپلیکیشن های وجود دارند که از ستندرد OpenPGP استفاده می نمایند، بناءً تمام کاربران نیاز ندارند که دقیقاً از عین برنامه استفاده کنند، اما آنها باید با " کلید های تبادله" مجهز باشند. قبل آنکه ایمیل های رمزگذاری شده (encrypted) ارسال شود، باید در مورد بهترین روش تامین ارتباطات مصون با مخاطبین تماس حاصل نمایید.

Mailvelope یک برنامه توصیه شده است که می تواند با ارائه کنندگان معروف خدمات ویبمیل (webmail) مانند Gmail، Outlook، Hotmail و Yahoo مورد استفاده قرار گیرد. می توان آنرا به عنوان یک افزونه (extension) در مرورگر (browser) های چون Google Chrome و Firefox علاوه نمود. این برنامه باعث ایجاد یک جوره کلید عامه و خصوصی مورد نیاز می شود، سپس کلید عامه را با سایر کاربران در میان می گذارد، تا آنها آنرا علاوه نمایند.

ب. اطلاعات را به گونه مصون ذخیره و جابجا نمایید

کاربران باید نه تنها اطلاعاتی را که با دیگران در میان می گذارند رمزگذاری (encrypt) نمایند، بلکه باید اطلاعات خود را نیز به منظور ذخیره مصون رمزگذاری (encrypt) کنند. این بخش رهنمایی در مورد روش های مختلف استفاده از رمزگذاری (encryption) برای ذخیره سازی دیتا در دستگاه های کاربران و در فضای ابری (cloud) می باشد.

ذخیره کردن تصاویر، ویدیو ها و دیتا در دستگاه:

Tella یک نمونه از اپلیکیشن های است که ما را در حفظ امنیت دیتا یاری می رساند. معمولاً از آن فعالان، مدافعان حقوق بشر، نهاد های جامعه مدنی، رسانه ها و کارشناسان امور بشردوستانه و مستندسازی، استفاده می نمایند. در حال حاضر، صرف برای دستگاه های Android قابل دسترس می باشد، اما نسخه iOS آن در حال انکشاف قرار دارد.

- طرز استفاده آن آسان است، چون از یک اتصال ساده برخوردار می باشد.
- کاربران از طریق ایجاد یک شکل، اپلیکیش را از طریق "روش نمونه" (pattern method) قفل می نمایند.
- کاربران می توانند ایکن (icon) اپلیکیشن را تغییر دهند، بناءً نمی توان آن را به آسانی شناسایی نمود.
- از ویژگی "حذف سریع" (quick delete) برخوردار می باشد، و در صورتیکه کاربران با خطر ضبط/مصادره تیلفون همراه شان روبرو باشند، می توان از آن به منظور حذف نمودن دیتا استفاده نمود.
- در صورت مواجه شدن با خطر فوری، اپلیکیشن می تواند خود به خود به شکل دایمی حذف شود.

رمزگذاری (Encrypting) و ذخیره سازی فایل ها با استفاده از خدمات ابری (cloud services)

هرچند، اکثریت افراد فایل های حساس شان را در کمپیوتر یا هارد دیسک های خارجی (بدون آنکه آنرا رمزگذاری نمایند) ذخیره سازی می نمایند، اما این یک روش خطرناک می باشد. هرگاه یک دسترسی غیرمجاز واقع شود، این دستگاه ها می تواند گرفته شوند و رمزگشایی (decrypted) شوند، یا اینکه برخی از افراد می توانند کاربران را وادار سازند تا رمزگذاری (encryption) را باز نمایند.

خیلی ها حایز اهمیت است که نباید اطلاعات حساس در دستگاه ها باقی بمانند، زیرا می تواند کاربران را هم به صورت آنلاین و هم به صورت آفلاین با خطر معروض سازند. ذخیره سازی مصون اطلاعات در ابر (cloud) متضمن اینست که اشخاص ثالث و غیرمجاز نتوانند به اطلاعات حساس دسترسی داشته باشند. باید کاربران از به جا گذاشتن نشانه/رد پا از دیتا در دستگاه های که می تواند سبب ایجاد مشکلات امنیتی شود، جداً خودداری نمایند.

"خدمات ابری" (Cloud services) عبارت از پلاتفورم های زیربنایی و یا نرم افزاری می باشند که توسط ارائه کنندگان ثالث میزبانی شده و از طریق انترنت در دسترس کاربران قرار می گیرند.

خدمات ابری (Cloud services) مصون ذیل برای ذخیره سازی اطلاعات حساس بدون به جا گذاشتن نشانه/رد پا های فزیکی توصیه می شود:

- Google Drive
- pCloud

هنوز هم مهم است که قبل از آپلود نمودن دیتا به ابر (cloud) باید رمزگذاری (encrypt) شود.

نرم افزار رمزگذاری (Ecryption software)

VeraCrypt: برنامه VeraCrypt در زمان نشر، یک برنامه منبع باز (open source) مصون پنداشته شده است، که دیتا را رمزگذاری (encrypt) نموده و فایل ها را در کمپیوتر کاربران ذخیره می نماید. صرف کاربران می توانند با استفاده از یک کلید رمزگشایی (decrypt) دیتا را مشاهده نمایند. برنامه VeraCrypt از یک سو می تواند دیتا، فایل ها و فولدر ها را رمزگذاری (encrypt) نماید، از سوی دیگر می تواند تمام دستگاه های خارجی مانند درایف های فلش USB، هارد دیسک ها یا قسمت های از هارد درایف را رمزگذاری (encrypt) نماید. از این برنامه می توان در ویندوز، Mac وLinux استفاده به عمل آورد.

VII. دیتا را به گونه مصون حذف نمایید

زمانیکه کاربران دیتا را از کمپیوتر، تیلفون هوشمند، کمره دیجیتال و یا دستگاه های دیگر "حذف" می نمایند، در حقیقت دیتا مذکور به کلی از بین نمی رود. گزینه حذف (Deletion) به سادگی دیتا را از کاربر "پنهان" (hide) می نماید، اما آنرا از دستگاه پاک سازی نمی کند.

در این بخش در مورد چگونگی پاک سازی مصون و دائمی دیتا توضیحات ارائه شده است و اصطلاحات اساسی مرتبط با اسکن امنیتی، چگونگی اجرای پروسه، و اینکه از برنامه ها و اپلیکیشن های مصون چگونه می توان به منظور پاک سازی اطلاعات، طوری که دگر بازیابی شده نتواند، را تحت پوشش قرار می دهد.

نفهمیدن تفاوت میان این اصطلاحات کلیدی مهم است.

حذف کردن (Deleting)

زمانیکه یک مدرک از یک دستگاه **"حذف"** (delete) می شود، به آسانی "پنهان" (hide) می شود. موجودیت آن به کلی حذف نشده و می توان آن را بازیابی (recover) نمود.

"مرا پنهان کن، اما اگر واقعاً به بازیابی من نیاز داشته باشی همینجا خواهم بود".

پاک کردن (Erasing)

پاک کردن دیتا سبب **"مفقود شدن"** (missing) آن در سیستم عملیاتی می شود. اکثراً قبل از آنکه دیتا پاک شود، کاربران در مورد اینکه دیتا قابل بازیابی (recover) نخواهد بود، هشدار های قبلی دریافت می کنند. از آنجاییکه سیستم عملیاتی نمی تواند دیتا را مشاهده نماید، زمانیکه محتویات درایف دیده شود، خالی به نظر می رسد. دیتا می تواند از طریق "پاک سازی" (wiping) یا "پارچه کردن" (shredding) پاک شود.

"مطمین هستی؟ دیگر هیچگاه مرا نخواهی دید! ".

پاک سازی (Wiping)

زمانیکه یک هارد دیسک یا دستگاه ذخیره سازی **"پاک سازی"** (wipe) می شود، تمام مدارکی که در آن موجود است، به شمول تمام مدارکی که کاربران قبلاً آنرا حذف نموده اند و هنوز قابل بازیابی اند، پاک می شوند.

"هر چیز را از بین خواهم برد ".

پارچه کردن (Shredding)

زمانیکه یک بخشی از دیتا (معمولاً یک یا چند فایل یا فولدر) **"پارچه"** (shred) می شود"، صرف قلم (اقلام) مشخصاً انتخاب شده پاک می شوند، نه اقلام دیگر.

"می خواهم فقط و فقط اینرا پاک نمایم".

پرسش های مکرر/معمول:

پرسش	
آیا حذف کردن (delete) فایل ها از desktop و تخلیه Recycle Bin به معنای حذف دائمی و غیرقابل برگشت آنها از کمپیوتر یا تیلفون هوشمند می باشد؟	
نخیر	بلی

نخیر، حذف کردن (delete) دیتا و تخلیه Recycle Bin، ظرفیت/فضای موجود را به عنوان "قابل دسترس" علامت گذاری می نماید، اما تا زمانیکه روی اطلاعات جدید "ظرفیت/فضای قابل دسترس" نوشته شود، هنوز هم می توان دیتای مربوطه را بازیابی (recover) نمود.

پرسش

آیا فارمت کردن مجدد (reformatting) هارد دیسک دیتا را به گونه دایمی و غیرقابل برگشت حذف می نماید؟

نخیر | بلی

نخیر، فارمت کردن مجدد (reformatting) یکی از روش های عالی برای "حذف کردن" (delete) دیتا به شمار می رود، نه "پاک کردن" (erase) آنها! پروسه فارمت کردن مجدد (reformatting)، تمام ظرفیت/فضای دستگاه را به عنوان "قابل دسترس" علامت‌گذاری می نماید. اما هنوز هم می توان دیتای مربوطه را بازیابی (recover) نمود، تا زمانیکه روی آن اطلاعات جدید نوشته شود. هرگاه عین کاربر پلان داشته باشد که از درایف مورد نظر استفاده مجدد نماید، در آن صورت این یک پروسه قابل قبول است، اما به طور اتوماتیک اطلاعات حساس را حذف نمی کند.

تخنیک های بازیابی فایل های حذف شده با گذشت هر روز رشد نموده و شماری زیادی از انواع فایل های ظاهراً "حذف شده" (deleted) مانند (تصاویر، اسناد ویدیو ها و غیره) قابل بازیابی می باشند. پاک سازی (Wiping) یا پارچه کردن (Shredding) دیسک به ما اطمینان می دهد که ظرفیت/فضای "قابل دسترس" ایجاد شده توسط حذف ساده، بازنویسی می شود و دیتای مربوطه را غیرقابل بازیابی می سازد.

چگونه می توان دستگاه ها را پاک سازی نمود؟

برای پاک سازی کمپیوتر (ویندوز)، (حذف نمودن فایل های موقت و پاک کردن فایل های سیستم)، از **ابزار پاک سازی دیسک (Disk Cleanup tool)** به شکل ذیل استفاده به عمل آورید:

- ابتدا به مینوی Start، سپس به گزینه All Programs، متعاقب آن به گزینه System Tools بروید، بعداً گزینه "Disk Cleanup" را انتخاب نمایید (و یا "Disk Cleanup" را در جعبه جستجو تایپ نمایید، تا موقعیت برنامه را باز نماید).

چگونه می توان دیتا را به شکل دایمی پاک سازی نمود؟

یکی از عناصر عمدۀ پاک سازی دیتا عبارت از پاک سازی لایه های مربوطه اطلاعات و بازنویسی آنها با دیتا های جدید می باشد. این کار به صورت دایمی از احتمال بازیابی دیتا جلوگیری می نماید.

- Eraser:پاک کننده یک ابزار امنیتی برای ویندوز است که به شما امکان می دهد اطلاعات حساس را به طور کامل از هارد دیسک خود حذف کنید.
- BCWipe: برنامه ای برای پاک کردن و نابود کردن اطلاعات.

اگر سیستم کمپیوتر خود را دور می اندازید، توصیه می شود هارد دیسک و رم (RAM) را جدا کنید و به طور جداگانه و مصون از بین بروند زیرا می توانند حاوی دیتا باشند.

VIII. جلوگیری از فیشنگ (phishing)

"فیشینگ" (Phishing) که به نام های تقلب الکترونیکی، دستبرد الکترونیکی و سرقت الکترونیکی نیز مسمی می باشد، مجموعه ای از تخنیک ها و تکنیک های می باشد که به منظور سرقت نمودن یا دستیابی به اطلاعات شخصی، رمز، اطلاعات تجارتی، حسابات مالی و غیره، مورد استفاده قرار می گیرد.

فیشنگ (Phishing) یکی از مروج ترین روش های می باشد که کاربران را مورد هدف قرار می دهد، و جلوگیری از فیشنگ (Phishing) ساده‌ترین روشی می باشد که کاربران می توانند با استفاده از آن از قربانی شدن خود جلوگیری نمایند.

به زبان ساده می توان گفت که مهاجمان معمولاً از طریق یک پروسه فریب دهنده از کاربران سوء استفاده می کنند و یا اینکه از تخنیک های انجنیری اجتماعی برای ترغیب یا وادار کردن قربانی استفاده می نماید، ته به درخواست مهاجم پاسخ مثبت دهد. درخواست معمولاً بخاطر اینست که کاربران را متقاعد سازند تا:

- بالای لینک مورد نظر کلیک نمایند.
- اطلاعات را در میان بگذارند.
- اجازه بدهند.
- فایل های ملوث با نرم افزار های مخرب را دانلود نمایند.

مهاجم معمولا انتظار می کشد تا شخص مورد هدف یا قربانی مرتکب اشتباه شود، سپس می تواند به اطلاعات و حساب های وی دسترسی پیدا کند.

انواع فیشنگ (phishing)

فیشنگ (phishing) انواع مختلف دارد، مانند:

فیشنگ نیزه ای (Spear phishing)

عبارت از یک تخنیک مغلق بوده که یک فرد یا گروه مشخص را مورد هدف قرار می دهد. مهاجم اطلاعات مرتبط به قربانی را جمع آوری می نماید، سپس از آن برای طرح ریزی یک پیام استفاده به عمل می آورد که واقعی جلوه می کند. به صورت عموم، این نوع فیشنگ (phishing) از طریق ارسال ایمیل های که قربانی را مورد هدف قرار می دهند صورت می گیرد.

Whaling

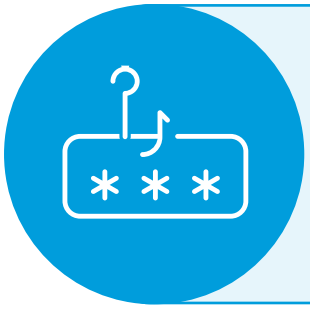
این نیز یکی از تخنیک های فیشنگ نیزه ای (Spear phishing) بوده، که افراد بانفوذ و قدرتمند را در شرکت ها یا نهاد ها مورد هدف قرار می دهد.

Pharming

یک نوع تقلب است که مهاجم با استفاده از آن شخص قربانی را از یک سایت اصلی/معتبر به سمت یک سایت جعلی دیگر و یا یک سایتی ملوث با نرم افزار های مخرب، هدایت می نماید. سپس، زمانیکه قربانی در سایت مورد نظر وارد می شود، می تواند اطلاعات قربانی رهگیری شود.

Smishing

عبارت از استفاده از پیام های کتبی (SMS) به منظور فریب دادن قربانی می باشد، که عمدتاً قربانی را ترغیب می کند تا اطلاعات مرتبط به حساب ها را افشا نماید، شماره های احراز هویت چندعاملی (MFA) را دریافت نماید و یا نرم افزار های مخرب را در دستگاه خویش دانلود نماید.



فیشنگ انجن جستجو (Search engine phishing)

در این نوع فیشنگ معمولاً مهاجم در انترنت یک ویب سایت ایجاد می کند و آنرا در انجن های جستجو یا رسانه های اجتماعی قرار می دهد و اجناس را با قیمت ارزان پیشکش می نماید و قربانی را ترغیب می نماید تا برای یک جنس پول بپردازد. سپس قربانی اطلاعات مرتبط با حساب بانکی خود را وارد می نماید، که بلافاصله به سرقت برده می شود و مورد استفاده قرار می گیرد.

فیشنگ صوتی (Voice phishing)

در این نوع فیشنگ مهاجم از تماس تیلفونی صوتی استفاده می کند، تا قربانی را فریب دهد که طوری تصور کند که شخص مورد نظر از یک مرجع رسمی تماس گرفته است، و بدین ترتیب اطلاعات مورد نظر را از قربانی به دست آورد.

چگونه می توان از خود در برابر فیشنگ (phishing) دیجیتال محافظت نمود؟

اطلاعات بیشتر در مورد فیشینگ و نمونه هایی از ایمیل های فیشینگ در اینجا قابل دسترس است.

باید تمام کاربران بی نهایت مواظب باشند و نکات ذیل را مدنظر بگیرند:

۱. **هیچگاه اطلاعات حساس و یا شخصی تان را با دیگران در میان نگذارید** و به هیچ وجه و در هیچگونه شرایط آنرا در شبکه های اجتماعی نشر نکنید.

۲. **در هیچگونه شرایط به تهدیدات دریافت شده** از طریق پیام ها، ایمیل ها و یا سایت های شبکه های اجتماعی، **پاسخ ندهید**. به هیچ صورت با تهدید کنندگان تعامل نکنید.

۳ **هیچگاه لینک ها را که** حتی از مخاطبین نزدیک خویش **دریافت می نمایید**، بدون بررسی قبلی **باز نکنید.**

الف. از برنامه Virus Total به منظور بررسی لینک ها و فایل ها استفاده به عمل آورید. پس از آنکه یک لینک را دریافت نمودید، بلافاصله بالای آن کلیک نکنید، بلکه لینک مذکور را کاپی نموده ویب سایت را باز نمایید و لینک را در ویندوز "URL Links" پیست (paste) نمایید و آنرا "Enter" کنید. هرگاه نتیجه آن 0 باشد، در آن صورت لینک عاری از بدافزار (malware-free) می باشد. هیچگاه مستقیماً بالای لینک کلیک نکنید، بلکه آنرا کاپی نموده و در مرورگر (browser) پیست (paste) نمایید. هرگاه لینک مذکور از محتویات نارمل برخوردار باشد، در آن صورت محتویات آن در مرورگر(browser) ظاهر می شود.

٤ **اطمینان حاصل نمایید که سایت های که به آنها دسترسی دارید از گواهینامه امنیتی برخوردار هستند و لینک مورد نظر با "https://" شروع شده است.** موجودیت یک آیکن قفل در مجاورت URL در آدرس بار مرورگر (browser's address bar) بدین معناست که SSL از ویب سایتی که کاربر از آن بازدید می نماید، محافظت می کند. SSL اتصالات انترنتی را مصون نگهداشته و به کاربران غیرمجاز اجازه نمی دهد تا اطلاعاتی را که بین دو سیستم تبادله می شود، بخوانند و یا آنرا تغییر دهند.

٥ **آدرس یا شماره تماس ایمیل ها و پیام های کتبی (SMS) را بررسی نمایید.** اکثراً مهاجمان آدرس ها خود را پنهان می نمایند، تا طوری به نظر برسند که گویا مخاطبین معتبر هستند، اما با بررسی دقیق تر مشاهده می شود که آنها با ویب سایت یا شخصی که وانمود می‌کنند، همخوانی ندارند.

٦ **تمام خدماتی که شما به خاطر دانستن نام تان آنرا سبسکرایب (subscribe) نموده اید، و نام شما در ارتباطات آنها وجود خواهد داشت.** هر پیامی که تحت عنوان "به سبسکرایب کننده محترم" (To our dear subscriber)، "مشتری عزیز" (kind customer) و یا شبیه آن ظاهر می شود، می تواند یک پیام تقلبی باشد: پس، برای رسیدگی به آن مواظب باشید.

٧ **هرگونه هدیه و یا جایزۀ که شما دریافت می کنید، تقلبی بوده می تواند**، بناءً در صورتیکه در مسابقه یا رقابتی شرکت نه ورزیده اید، از تعامل خوددارای نمایید.

٨ **هرگاه شما یک ایمیل و یا مکالمه دیگری دریافت نموده باشید که از شما خواستار اطلاعات حساس باشد، مستقیماً از یک طریق دیگر با فرستنده در مورد وضاحت پیام دریافت شده تماس حاصل نمایید.**

٩ از دستگاه های خود با استفاده از **برنامه های امنیتی انترنتی و ضد بدافزار (anti-malware) محافظت نمایید و هیچگاه در آنها نرم افزار های "کرک شده" (cracked) و یا سرقت شده را نصب نکنید.**

١٠ در تمام حساب **ها، تائید دو مرحله یی را فعال سازید.**

IX. ماخذ ها و مطالعه بیشتر

لطفاً جهت دریافت معلومات مزید، منابع و معلومات تازه، به ماخذ های ذیل مراجعه نمایید:

۱. **رهنمود مصونیت دیجیتلی برای افغانستان** (دری): این رهنمود خطر، مراحل پیشگیری، مراحل پاسخ و اخذ تصامیم مهم را به بررسی میگیرد.

۲. **منابع ایمنی آنلاین برای مدافعین حقوق بشر افغانستان** (دری): این معلومات به شما کمک می کند تا در تشدید بحرانها به امنیت آنلاین خود بهبود بخشید.

۳. **امنیت رسانه های اجتماعی** (دری): معلومات در مورد امنیت تیلیفون های هوشمند و اپلیکیشن های پیام رسانی.

٤. **ایجاد رمز نیرومند** (دری): معلومات در مورد مراحل ایجاد رمز نیرومند.

٥. **امنیت مرورگر** (دری): مرورگرها ها را چطور به حالت ناشناس تبدیل نمائیم، از کدام مرورگرها استفاده نمائیم و توصیه های لازم دیگر در مورد استفاده از VPN.

٦. **شناسایی خطرات** (دری): چگونه می توانید در فضای مجازی مراقب خود باشید.

۷. **جلوگیری از سو استفاده از معلومات های بیومتریک** (دری): باید و نبایدها هنگام بایومتریک.

۸. **شیوه ها برای امنیت دیجیتالی** (دری): معلومات درباره چگونگی پنهان نمودن مکان، امنیت داده ها و اطلاعات، محافظت در مقابل بدافزارها و خدمات ذخیره سازی آنلاین فایل ها.

۹. **حذف تاریخچه دیجیتال** (دری): معلومات در مورد حذف نمودن حساب ایمیل و رسانه های اجتماعی و امن سازی حساب های موجود.

۱۰. **انقطاع و مسدود شدن انترنیت** (دری): معلومات درباره استفاده از VPN و تماس مصون در صورت قطع کلی انترنت.

۱۱. **رهنمود برای فعالان جامعه مدنی** (دری): معلومات در مورد دادخواهی در محیط های پرمخاطره.

۱۲. **مدافعین صف مقدم** (دری): معلومات و حمایت در مورد خطرات دیجیتالی و سایر خطرات امنیتی برای مدافعان حقوق بشر.

۱۳. **امنیت در داخل یک جعبه " Security-in-a-Box "** (دری): معلومات امنیت دیجیتالی، رهنمود های آموزشی و منابع دیگر.

۱٤. **دفاع شخصی نظارت یا سرویلانس** (پشتو) نکات، ابزار ها و چگونگی تامین ارتباطات آنلاین مصون، که توسط بنیاد مرز الکترونیکی (Electronic Frontier Foundation) راه اندازی می شود.

۱٥. **شماره های تماس هنگام حادثه امنیت دیجیتالی** (انگلیسی): پاسخ سریع هنگام حادثه امنیت دیجیتلی.

X. همکاری های عاجل (Emergency Assistance)

لطفا جهت دریافت همکاری در حالت اضطراری به آدرس های ذیل مراجعه نمائید.

۱. مدافعین صف مقدم: (انگلیسی) Emergency Contact | Front Line Defenders

۲. گزارشگران بدون مرز: (دری) تماس با ما | RSF

۳. کمیته مصونیت خبرنگاران افغان: Dari | Afghan Journalists Safety Committee (safety-committee.org)

٤. پنجره تمویل مالی صندوق بشردوستانه و صلح زنان (WPHF) برای زنان مدافع حقوق بشر (WHRDs): Dari | Afghan Journalists Safety Committee (safety-committee.org)

٥. صندوق واکنش به بحران، کمک های مالی فوری به فعالان جامعه مدنی: (انگلیسی) Crisis Response Fund (civicus.org)

٦. میکانیزم مدافعان حقوق بشر- اتحادیه اروپا: (انگلیسی) ProtectDefenders.eu - You have the right to defend rights

XI. مصطلحات امنیت سایبری (cybersecurity)

تعریفات ذیلاً ارائه شده را می توان در دیتابیس مصطلحات سازمان ملل متحد (UNTERM) که در اینجا قابل دسترس است، دریافت نمود، مگر اینکه طوری دیگر ارائه شده باشد.

- **نرم افزار تبلیغاتی مزاحمت کننده (Adware):** عبارت از یک نوع اپلیکیشن نرم افزار می باشد که حین راه اندازی، یک نوع تبلیغات را به نمایش می گذارد. بعضاً، تهیه کنندگان یک نسخه "رایگان" نرم افزار خود را ارائه می نمایند، به شرط اینکه شما وادار شوید تا تبلیغات را مشاهده نمایید، آنها همزمان با آنکه یکعده افراد بالای تبلیغات کلیک می نمایند، پول دریافت می کنند. در اکثر موارد عین نرم افزار از یک نسخه فروشی نیز برخوردار است، که عاری از تبلیغات می باشد.

- **حافظه پنهان (Cache):** عبارت از یک ساحه ذخیره سازی موقت بوده،که در آن دیتای که مکرراً به آن دسترسی صورت می گیرد، می تواند به منظور دسترسی سریع ذخیره شود.

- **نرم افزار کرک شده (Cracked software):** برنامه " crack" و یا " patch" عبارت از برنامهٔ می باشد که به منظور فعال ساختن، ثبت و راجستر و یا تمدید دوره آزمایشی یک برنامه اختصاصی طراحی شده است و معمولاً برای جلوگیری از سرقت و استفاده غیرمجاز به شماره مسلسل نیاز دارد. استفاده از " برنامه " crack" و یا " patch" به منظور دسترسی به برنامه های نرم افزار، همیشه غیرقانونی پنداشته می شود.[٥]

٥ لطفاً در ویکیپیدیا به (Software cracking - Wikipedia) مراجعه نمایید.

- **تکنالوژی رمزگذاری (Encryption technology):** کاربران را قادر می سازند تا از دیتای ذخیره شده در درایف های USB، دستگاه های تیلفون همراه، دیسک های فلش، پین درایف ها، سی دی و هارد دیسک ها محافظت نمایند. گیرندگان ناخواسته نمی توانند یک اسناد رمزگذاری شده (encrypted document) را بخوانند و یا مشاهده نمایند، ولو اگر آنها خود اسناد را نیز در اختیار داشته باشند.

- **رمزگذاری انتها - به - انتها "E2EE" (End-to-end):** عبارت از اپلیکیشن رمزگذاری (encryption) برای ابزار ها و خدمات ارتباطات می باشد، طوری که صرف استفاده کنندگان ابزار یا خدمات به پیام های کتبی ساده دسترسی دارند. عده کثیری از انواع رمزگذاری (encryption) توسط ارائه کنندگان خدمات به منظور مصونیت ارتباطات طوری مورد استفاده قرار می گیرند که از دسترسی غیرمجاز شخص ثالث جلوگیری می نماید، اما ارائه کننده خدماتی که آن را تطبیق می نماید هنوز می تواند به دیتای کاربران ذیربط دسترسی داشته باشد. رمزگذاری انتها - به - انتها "End-to-end"، به رمزگذاری اطلاق می شود که از آن نیز جلوگیری می نماید.

- **فایروال (Firewall):** فایروال عبارت از یک سیستمی می باشد که به منظور جلوگیری از دسترسی غیرمجاز به یک شبکه خصوصی و یا از یک شبکه خصوصی، طرح ریزی گردیده است. فایروال ها را می توان هم در سخت افزار و هم در نرم افزار و یا هم مشترکاً در هردوی آنها تطبیق نمود.

- **آدرس IP:** عبارت از یک شماره مشخص است که دستگاه های تکنالوژی معلوماتی از آن به منظور شناسایی و تامین ارتباط با یکدیگر در داخل یک شبکه کمپیوتری، با استفاده از ستندرد های پروتوکول انترنت (IP) استفاده می نمایند. هر دستگاه شبکه شرکت کننده، مانند روتر ها (routers)، کمپیوتر ها، پرنتر ها، دستگاه های فکس انترنتی، باید از یک آدرس مشخص برخوردار باشند. آنرا می توان معادل یک آدرس جاده یا یک شماره تیلفون تصور نمود که برای کمپیوتر یا سایر دستگاه های شبکه در انترنت مدنظر گرفته می شود. همانطور که هر آدرس جاده و شماره تیلفون مشخصاً یک ساختمان یا تیلفون را شناسایی می نماید، یک آدرس IP نیز می تواند یک کمپیوتر مشخص یا دستگاه شبکه دیگری را در یک شبکه شناسایی نماید.

- **Keylogger:** عبارت از یک ابزاری می باشد که فعالیت های کاربران مانند وارد کردن ضربه به کلید را ثبت می نماید و می تواند این معلومات را با استفاده از ایمیل یا طرق دیگر به مهاجم ارسال نماید.

- **نرم افزار مخرب یا "بدافزار" (Malicious Software or "Malware"):** عبارت از نرم افزاری می باشد که به منظور نفوذ یا صدمه زدن به یک سیستم کمپیوتری، بدون رضایت آگاهانه مالک طرح ریزی شده است. نرم افزار مذکور با در نظر داشت نیت و اراده مرجع تولید کننده بدافزار (malware) پنداشته می شود، نه به خاطر کدام ویژگی خاص آن. اینگونه نرم افزار شامل وایرس های (viruses) کمپیوتری، کرم ها (worms)، تروجان ها یا اسپ های تروجان (Trojan or Trojan Horse)، نرم افزار های جاسوسی (spyware)، ابزار های تبلیغاتی مزاحمت کننده غیرصادق (dishonest adware) و سایر نرم افزار های مخرب و ناخواسته می باشد. طوری که دیده می شود این اصطلاح از دو کلمه مخرب (malicious) و نرم افزار (software) ترکیب یافته است.

- **مسیریابی پیازی (onion routing):** بنیاد تکنالوژیکی شبکه Tor را تشکیل می دهد. این نام از ساختار پیاز مانندی که در طرح رمزگذاری (encryption) مورد استفاده قرار گرفته است، اقتباس شده است، که چندین مراتبه در لایه های متعدد مصون گردیده است. هدف از مسیریابی پیازی (onion routing) استفاده از انترنت با حفظ محرمیت ممکنه، مسیریابی (ترافیک) از طریق سرور های متعدد و رمزگذاری آن در هر مرحله می باشد.[٦]

- **نرم افزار منبع باز (Open source software):** این در واقع یک اصطلاح عمومی برای نرم افزار (نرم افزار اپلیکیشن و سیستم) می باشد، که در آن کد منبع به شکل آزادانه در اختیار تمام کاربران قرار دارد. یعنی یک برنامه ای که می توان از آن بدون هرگونه محدودیت در کاپی کردن، خواندن، تغییر دادن و پخش مجدد، استفاده نمود.

٦ لطفاً برای دریافت معلومات مزید به پروژه Tor در لینک (https://www.torproject.org) مراجعه نمایید.

- **PGP:** مخفف "Pretty Good Privacy" (محرمیت بسیار خوب) می باشد، که در واقع یک نرم افزار رمزگذاری کلید-عامه (public-key) غیرمتجانس بوده که از قابلیت حفظ محرمیت و سنخیت ارتباطات الکترونیکی برخوردار می باشد.

- **فیشنگ (Phishing):** عبارت از یک تخنیک تقلب آنلاین و سرقت هویت می باشد. مثلاً، یک "فیشر" (phisher) یک ایمیل را به عنوان یک درخواست تجارنی مشروع ارسال می دارد، به عنوان مثال، به نمایندگی از یک بانک از مشتریان می خواهد تا دیتا مالی را مودر تایید قرار دهند. ایمیل مذکور معمولاً حامل یک لینک می باشد که به نظر می رسد متعلق به یک ویب سایت بانکی مشروع می باشد. اما، در واقع سایت مورد نظر جعلی بوده و زمانیکه قربانی شماره حساب، رمز و یا سایر معلومات حساس را تایپ می نماید، دیتای مذکور جمع آوری می شود و بعداً توسط فیشر (phisher) به منظور تقلب مورد استفاده قرار می گیرد.

- **افزار باجگیری (Ransomware):** عبارت از یک نوع نرم افزار مخرب می باشد که به منظور این طراحی گردیده است که در صورت عدم پرداخت یک مقدار پول به کاربران اجاره نمی دهد که به سیستم کمپیوتری دسترسی داشته باشند. شماری از انواع افزار باجگیری (Ransomware)، فایل ها را در هارد دیسک سیستم رمزگذاری می نمایند (که به باجگیری ویروسی رمزنگاری شده یا "a.k.a. cryptoviral extortion " شهرت دارد)، حالانکه عدۀ دیگر آنها می توانند سیستم را به سادگی قفل نمایند و پیام های را به منظور وادار کردن کاربران به پرداخت پول به نمایش بگذارند.

- **نرم افزار جاسوسی (Spyware):** عبارت از نرم افزار کمپیوتری می باشد که بدون رضایت آگاهانه کاربران اطلاعات شخصی آنها را جمع آوری می نمایند. اطلاعات شخصی معمولاً به شکل مخفیانه با استفاده از تخنیک های گوناگون مانند ثبت ضربه های کلید، ثبت تاریخچه جستجوی انترنتی و اسکن نمودن اسناد در هارد دیسک کمپیوتر، ثبت می شوند.

- **تروجان ها یا اسپ های تروجان (Trojan or Trojan Horse)**، عبارت از یک برنامۀ می باشد که مشروع به نظر می رسد، اما حین راه اندازی دست به یکعده فعالیت های غیرقانونی می زند. می تواند به منظور تثبیت اطلاعات رمز و یا آسیب پذیرتر ساختن بیشتر سیستم در برابر وارد شدن آینده یا خیلی ساده به منظور از بین بردن نرم افزار و دیتای ذخیره شده توسط کاربران، مورد استفاده قرار گیرد. تروجان با وایرس شباهت دارد، با این تفاوت که خود را تکثیر نمی کند.

- **شبکه خصوصی مجازی (VPN):** "شبکه خصوصی مجازی" عبارت از یک شبکه ای می باشد که فراهم کنندۀ یک مسیر کنترول شده از طریق انترنت بوده و تنها کاربران مجاز به آن دسترسی دارند و از این مسیر صرف دیتا مجاز می توانند انتقال یابد.

- کرم ها **(Worms):** یک اصطلاح کمپیوتری بوده که به برنامه های پرازیت دار مخرب، شبیه وایرس ها، که از قابلیت تکثیر برخوردار بوده و در سراسر شبکه ها در جستجوی ملوث ساختن ماشین های آسیب پذیر می باشند، اطلاق می گردد. کرم ها (worms)، برخلاف وایرس ها، سایر فایل های برنامه کمپیوتری را ملوث نمی سازند. کرم ها (worms)، می توانند در عین کمپیوتر کاپی ها را ایجاد نمایند و یا می توانند کاپی ها را از طریق یک شبکه به کمپیوتر های دیگر ارسال نمایند.

UN Women Afghanistan Country Office
www.unwomen.org
www.unama.unmissions.org

UNAMA

UN WOMEN