بسته آموزشی امنیت دیجیتال

UNREPRESENTED
NATIONS & PEOPLES
ORGANIZATION
unpo.org

آموزش امنیت دیجیتال

بسته آموزشی امنیت دیجیتال

اطلاعات عمومی

زمان:

ما این مواد آموزشی را برای تکمیل در 4 ساعت آماده کرده‌ام

آنچه نیاز دارید:

برای استفاده مناسب از این سند، مربی به پاورپوینتی که برای ارائه اطلاعات عملی بیشتر و به اشتراک گذاری موثرتر اطلاعات تهیه شده است، نیاز دارد.

فعالیت‌ها:

در این جعبه ابزار ما فعالیت‌های کوتاهی را برای ارزیابی درک شرکت‌کنندگان و تقویت فرآیند یادگیری گنجانده‌ایم.

هدف:

این جعبه ابزار اطلاعات لازم را برای فعالان فراهم می‌کند تا به‌صورت آگاهانه از خطرات احتمالی سایبری به‌صورت آنلاین مرور کنند. در این سند شما نکات و ترفندهایی از کارشناسان پیدا خواهید کرد تا استراتژی خود را برای ادامه فعالیت‌های خود در حین پیشگیری در سفر دیجیتال خود توسعه دهید.

برای چه کسانی:

این ماژول برای سازمان‌های غیردولتی یا فعالان فردی که مایل به یادگیری امنیت دیجیتال برای فعالیت‌های روزانه خود هستند، طراحی شده است

چگونه از این جعبه ابزار استفاده کنیم:

بگو یا بپرس	
نشان بده	
فعالیت	
تعریف	
نکات عملی	

فهرست مطالب

اطلاعات عمومی

چگونه از این جعبه ابزار استفاده کنیم

بخش 1: خوش‌آمدگویی و مرور کلی

بخش 2: نگاهی به برخی از تئوری‌های امنیت دیجیتال

بخش 3: حفاظت از داده‌های شما در رایانه و تلفن همراه

الف) رمز عبور

ب) مدیر رمز عبور

ج) احراز هویت دومرحله‌ای

بخش 4: مرور اینترنت به‌صورت محرمانه

الف) استفاده از VPN

ب) مرورگر وب

بخش 5: حفاظت از خود در برابر فیشینگ و بدافزارها

بخش 6: اطمینان از ایمن بودن ارتباطات شما

بخش 7: امنیت تلفن هوشمند

بخش 8: نکات پایانی و سوالات متداول

بخش 1: خوش‌آمدگویی و مرور کلی

خوش‌آمدگویی:
به افراد خوش‌آمد بگویید و از آمدنشان تشکر کنید.

یخشکن: از افراد بپرسید
نام‌هایشان
برای چه فعالیت‌هایی از رایانه خود در زندگی روزمره استفاده می‌کنند
(چه نوع تلفن و رایانه‌ای دارند (بدون دادن جزئیات زیاد
آیا تاکنون درسی در زمینه امنیت سایبری گذرانده‌اند

اسلاید 1 را نشان دهید: درک اهمیت امنیت دیجیتال در عصر مدرن

بگویید: "ما از ابزارهای دیجیتال برای فعالیت‌های روزمره بیشتری استفاده می‌کنیم. ما شاهد رشد نمایی استفاده از نوعی از رایانه (اغلب یک تلفن هوشمند) برای کارهایی مانند خرید، روشن کردن یخچال، کمپین برای یک هدف، انجام تکالیف یا وظایف - و به طور فزاینده‌ای فناوری به گونه‌ای تکامل می‌یابد که همه این‌ها در یک جامعه دیجیتالی شبکه‌ای واحد قرار دارد. ما به دستگاه‌های دیجیتال در زندگی روزمره خود بسیار وابسته شده‌ایم که به تهدیدات دیجیتالی مانند شکایات، اخاذی، هک و موارد دیگر بسیار آسیب‌پذیر شده‌ایم .

بپرسید: این وضعیت فعالان را کجا قرار می‌دهد؟ بسیار آسیب‌پذیر

در اینجا چند مورد از حملات سایبری به فعالان آورده شده است :
الف) مورد گروه هکری ایرانی را ارائه دهید که از یک برنامه آموزشی گواهینامه رانندگی برای دسترسی به یک فعال استفاده کردند. نشان دهید که هکرها از اطلاعات شخصی برای دستیابی به نتایج استفاده می‌کنند از جمله تظاهر به شخص مورد نظر .

ب) در سال 2020، بدافزاری در یک برنامه گواهینامه رانندگی در سوئد شناسایی شد. به گفته امیر رشیدی، محقق گروه میان، یک سازمان حقوق بشری با تمرکز بر امنیت دیجیتال، این برنامه اقلیت‌های قومی و مذهبی را هدف قرار می‌دهد. هنگامی که برنامه نصب می‌شود، می‌تواند مکالمات، موقعیت مکانی و تاریخچه مرور را ضبط کند .

بگویید: این دوره‌ها فقط برای آموزش شما به عنوان یک حرفه‌ای در امنیت دیجیتال نیست، بلکه برای اطمینان از

اینکه شما و جامعه فعالان یا مردم شما از خطرات احتمالی سایبری آگاه هستید و پیشگیرانه با دقت به فعالیت‌های روزانه خود ادامه می‌دهید.

بخش 2: نگاهی به برخی از تئوری‌های امنیت دیجیتال

اسلاید اکس را نشان دهید: تعریف امنیت سایبری

بگویید: امنیت سایبری همه چیز در مورد حفاظت از دارایی‌های دیجیتال در برابر تهدیدات است. دارایی می‌تواند هر چیزی باشد که می‌خواهید محافظت کنید: دستگاه‌های فیزیکی شما مانند تلفن یا ساعت هوشمند که نمی‌خواهید در فرودگاه از شما دزدیده شود. اما اغلب دارایی‌هایی که به عنوان یک متخصص امنیت سایبری محافظت می‌کنید، داده‌ها هستند .

از مخاطبان بپرسید: چه نوع مهارت‌هایی را فکر می‌کنید یک شخص در زمینه امنیت سایبری دارد؟
پاسخ‌های آن‌ها را روی تخته بنویسید .

اسلاید اکس را نشان دهید

واقعیت این است که امنیت سایبری یک حوزه چندرشته‌ای است - و بر خلاف جیمز باند شما نمی‌توانید در همه چیز متخصص باشید - زیرا یک سیستم گسترده و پیچیده است. در حوزه امنیت سایبری شامل موارد زیر می‌شود :

- امنیت زیرساخت‌های حیاتی
- امنیت برنامه‌ها
- امنیت شبکه
- امنیت ابر
- امنیت اینترنت اشیا (IoT)
- و بسیاری موارد دیگر

در این جلسه، ما به هر یک از این زیرشاخه‌های امنیت سایبری نخواهیم پرداخت، بلکه شما درک بهتری از کل حوزه خواهید داشت که به شما امکان می‌دهد نگرانی‌های خود را به افراد مربوطه ارجاع دهید .

از مخاطبان بپرسید: تفاوت بین داده و اطلاعات چیست؟

هکر اغلب نگران پردازش داده‌ها نیست. مانند متخصص امنیت سایبری، او جیمز باند نیست، چندین کار انجام نمی‌دهد، کار او استخراج داده‌ها و سپس یا تحویل آن به سرورهای خود برای پردازش یا فروش آن به شخص دیگر برای پردازش است. بنابراین هنگامی که در مورد داده صحبت می‌کنم، آن را به عنوان اطلاعات خامی که هنوز پردازش نشده است در نظر بگیرید.

هنگامی که اهمیت حفاظت از دارایی‌ها، به ویژه داده‌ها را درک کردید، بیایید نگاهی به مثلث CIA داده‌ها بیندازیم، که نباید با آژانس اطلاعات مرکزی (CIA) اشتباه گرفته شود .

مثلث CIA یا محرمانه‌بودن، یکپارچگی و دسترسی یک مدل امنیتی است که برای هدایت افراد و سیاست‌ها برای امنیت اطلاعات طراحی شده است .

اسلاید 3 را نشان دهید: محرمانه‌بودن، یکپارچگی و دسترسی

- **محرمانه‌بودن**: حفظ داده‌ها از تلاش‌های عمدی یا غیرعمدی برای دسترسی به آن‌ها برای مشاهده.
- **یکپارچگی**: اطمینان از اینکه داده‌ها به‌طور عمدی توسط هیچ عاملی تغییر نمی‌کنند.
- **دسترسی**: اطمینان از اینکه داده‌های شما در همه زمان‌ها و به‌راحتی، با احترام به یکپارچگی آن، قابل دسترسی هستند .

بپرسید: تفاوت بین امنیت و حریم خصوصی در امنیت دیجیتال چیست؟

حریم خصوصی به توانایی شما برای کنترل، دسترسی و تنظیم اطلاعات شخصی یا اطلاعات سازمانی که برای آن کار می‌کنید، اشاره دارد .

امنیت به کل سیستم که داده‌ها را از تهدیدات محافظت می‌کند، اشاره دارد .

شما می‌توانید در یک محیط بسیار امن با حریم خصوصی ضعیف باشید زیرا داده‌های شما همچنان سالم می‌مانند و دزدیده نمی‌شوند، اما ارائه‌دهنده می‌تواند هر زمان که بخواهد نگاهی به آن بیندازد .

فعالیت: بیایید یک تمرین انجام دهیم که ماهیت تحلیل امنیت سایبری را تشکیل می‌دهد، یعنی تعریف دارایی‌ها، دشمنان، منابع در دسترس، احتمال حمله و توانایی‌های شما

یک چارچوب نهایی برای تحلیل :

از شرکت‌کنندگان بپرسید: سوالات زیر را در مورد تنظیمات دیجیتال خود و اینکه با کدام بازیگران باید مراقب باشند، مرور کنند.

- **مدارایی‌ها**: چه چیزی را باید محافظت کنم؟
- **دشمن:** از چه کسی؟
- **منابع:** دشمن من چه منابعی دارد؟
- **احتمال:** احتمال اینکه دشمن من من را هدف قرار دهد چقدر است؟
- **توانایی:** تا چه حد می‌خواهم برای محافظت از دارایی‌های خود پیش بروم؟

بخش 3: محافظت از داده‌هایتان روی کامپیوتر و گوشی موبایل

الف) رمزهای عبور

رمز عبور یک کلمه یا عبارت محرمانه است که باید برای ورود به یک مکان استفاده شود .

مهم‌ترین شکل محافظت از داده‌های شما، رمز عبور کاربری شما برای ورود به دستگاهتان است. این امر به طور حتم یک رشته کامل از روش‌های پیچیده برای رمزگذاری و رمزگشایی داده‌ها و پیام‌ها را ایجاد می‌کند تا آن‌ها را مخفی نگه دارد. این رشته به عنوان رمزنگاری شناخته می‌شود و هزاران سال است که وجود دارد و برای درک امنیت سایبری ضروری است. اگرچه ما به مشکلات ریاضی پیچیده‌ای که رمزنگاری ایجاد می‌کند نمی‌پردازیم، اما از خود می‌پرسیم چه چیزی یک رمز عبور خوب را می‌سازد.

از مخاطبان بپرسید: چه چیزی یک رمز عبور خوب را می‌سازد؟ چه چیزی یک رمز عبور بد را می‌سازد؟

پاسخ‌های احتمالی :

- چیزی که به زندگی شخصی شما مربوط نباشد (مثلاً نام سگتان یا تیم فوتبال مورد علاقه‌تان)

- چیزی که تنها یک یا دو کلمه باشد، زیرا این‌ها اغلب قابل حدس زدن هستند
- استفاده از کاراکترهای مختلف مثل حروف بزرگ، اعداد یا نمادها
- غیرقابل فهم بودن؟
- به‌طور ایمن ذخیره و محافظت شده باشد!
- یک رمز عبور خوب باید به خاطر سپردنی باشد

نمایش:

رمزهای خوب و بد		
خیلی خوب	بهتر	خیلی بد
j5LyF*H6IIg	Cynthia1970!	password
7+n*7XonGS	LayC70!	admin
VJ(>0WuVE83V	*cynthia70lay	cynthia
R.xzVv2m0R0;	CynthiaL7019	cynthialay

چه چیزی یک رمز عبور خوب را می‌سازد؟

طول :

بگویید: مهم‌ترین متغیر در تعیین قوت رمز عبور، طول آن است. این به‌طور قطع مهم‌ترین متغیر است و باید برای همه روشن شود. داشتن یک جمله به عنوان رمز عبور که طولانی باشد، ایمن‌تر از یک رمز عبور 5 کاراکتری با کاراکترهای مختلف است. یکی از دلایل آن این است که داشتن یک رمز عبور طولانی می‌تواند از تلاش هکر برای شکستن رمز عبور جلوگیری کند. دیگری این است که اگر هکر از هوش مصنوعی برای باز کردن رمز عبور به روش "حمله بی‌رحمانه" استفاده کند، به احتمال زیاد رمز عبور 5 کاراکتری را آسان‌تر می‌تواند شکسته کند.

پیچیدگی :

بگویید: بیشتر ما هنگام ایجاد رمز عبور از کلمات و شاید عدد استفاده می‌کنیم. اما این رمز عبورها به دلیل نرم‌افزارها و ابزارهای جدیدی که تمامی کلمات شناخته شده را آنی بررسی می‌کنند، بیشتر و بیشتر قابل شکستن

هستند. این نرم‌افزارها اغلب از هوش مصنوعی استفاده می‌کنند. به همین دلیل همیشه بهتر است از یک سری حروف تصادفی به جای یک کلمه استفاده کنید .

کاراکترهای ویژه :

بگویید: استفاده از کاراکترهای ویژه مانند: @ $ % & رمز عبور را بسیار ایمن‌تر و سخت‌تر برای حدس زدن می‌کند. امروزه، برخی وب‌سایت‌ها از شما می‌خواهند از کاراکترهای ویژه استفاده کنید تا رمز عبورتان معتبر باشد، اما متاسفانه نه همه وب‌سایت‌ها .

بگویید: **بدترین رمز عبوری** که می‌توانید استفاده کنید یک کلمه تنهاست. از آنجا که یک هکر می‌تواند از آنچه به عنوان حمله دیکشنری شناخته می‌شود برای شکستن رمز عبور شما استفاده کند. یک حمله دیکشنری می‌تواند روی یک کلمه کار کند. همین‌طور تاریخ تولدها، نام‌ها یا حتی "123456789"

بزرگترین مشکلی که ما داریم این است که در عصر مدرن بسیاری از رمزهای عبور برای حساب‌های مختلف و دستگاه‌های خود داریم. علاوه بر این، اگر اطلاعات حساس دارید، می‌خواهید هارد درایو و ذخیره‌سازی ابری خود را با یک رمز عبور قوی 36 کاراکتری رمزگذاری کنید که به راحتی به خاطر نمی‌سپارید. راه‌حل این مشکل استفاده از مدیر رمز عبور است.

ب) مدیر رمز عبور

نمایش اسلاید: لیست مدیران رمز عبور

مدیر رمز عبور به افراد و شرکت‌ها اجازه می‌دهد تا همه رمزهای عبور خود را از یک مکان ایمن ذخیره و مدیریت کنند. بنابراین، کاربران دیگر نیازی به یادآوری رمزهای عبور متعدد نخواهند داشت .

تفاوت بین مدیران رمز عبور می‌تواند در محدوده قیمت‌ها متفاوت باشد، اما همچنین اینکه رمزهای عبور شما کجا ذخیره می‌شوند. به عنوان مثال، Bitwarden رمزهای عبور شما را به نسبت ایمن در یک ابر روی سرورهای خود ذخیره می‌کند و به چندین نفر اجازه می‌دهد به حساب‌های مختلف دسترسی داشته باشند. اما ممکن است به هر دلیلی به Bitwarden اعتماد نداشته باشید و بخواهید داده‌های خود را به صورت محلی ذخیره کنید. KeyPassXC نمونه خوبی از یک مدیر رمز عبور با ذخیره‌سازی محلی است .

داشتن یک عبارت عبور برای دسترسی آسان به مدیر رمز عبور خود مهم است، اما بیایید نگاهی به یک لایه دیگر امنیتی بیندازیم: 2FA (تایید هویت دو مرحله‌ای) .

ج) تایید هویت دو مرحله‌ای (2FA)

تایید هویت دو مرحله‌ای، یا 2FA، یک لایه اضافی از محافظت است که برای اطمینان از امنیت حساب‌های آنلاین شما بیش از یک نام کاربری و رمز عبور استفاده می‌شود .

شما می‌توانید از دو روش احراز هویت کنید :

- چیزی که می‌دانید (مانند رمز عبور)
- چیزی که دارید یا همراه شماست (بیومتریک)

خبر خوب این است که شما می‌توانید و باید هر دو را استفاده کنید. با 2FA می‌توانید اطمینان حاصل کنید که حتی اگر یک هکر رمز عبور شما را بشکند، شما همچنان آن لایه اضافی امنیتی را دارید. این اغلب به شکل :

- یک اپلیکیشن روی گوشی شما که یک کد موقتی برای دسترسی به سرویس می‌دهد (مانند: Google Authenticator)

- یک کلید USB مانند Yubikeys یا Nitrokeys که هنگام اتصال می‌تواند کدهای بالا را به شما بدهد یا از طریق لمس یا حتی اثر انگشت شما امکان دسترسی به حساب شما را فراهم کند.

تایید هویت دو مرحله‌ای، یا 2FA، به سرعت در حال تبدیل شدن به یک اقدام اساسی در امنیت دیجیتال است. اکثر حساب‌های رسانه‌های اجتماعی اکنون اجازه تایید هویت دو مرحله‌ای، یا 2FA را می‌دهند و شما باید به محض اینکه این کلاس را ترک کردید، سیستم تایید هویت دو مرحله‌ای، یا 2FA، را در اکثر حساب‌های ایمیل، پیام‌رسانی و رسانه‌های اجتماعی خود اجر کنید.

.

محافظت از هارد دیسک و سیستم‌های ذخیره‌سازی ابری:

علاوه بر رمزگذاری هارد دیسک خود، از یک هارد دیسک خارجی برای سیستم‌های ابری که تأیید شده‌اند مانند Google Cloud، OneDrive استفاده کنید ...

استراحت

قسمت 4: مرور اینترنت به صورت محرمانه

اینترنت به عنوان راهی برای غیر متمرکز کردن ارتباطات و اتصال یک نفر به صفحه وب دیگری اختراع شد. این تکنولوژی به یک غول بزرگ تبدیل شده است که

داشتن دانش از موارد زیر قبل از شروع به مرور ایمن ضروری است :

- ارائه‌دهنده خدمات اینترنتی شما کیست؟
- ماهیت آدرس IP شما چیست؟ آیا ثابت است یا تغییر می‌کند؟ آدرس IP شما مانند شناسایی‌کننده شما برای شبکه خانگی یا کاری شماست
- تنظیمات فایروال شما چیست که رابطه IP شما را با سایر IP های موجود در وب جهان‌گستر تنظیم می‌کند (فکر کنید مانند یک سیاست کنترل مرزی برای کسانی که وارد و خارج می‌شوند)

الف) استفاده از فیلتر شکن (VPN)

بپرسید: آیا کسی می‌تواند توضیح دهد که فیلتر شکن چیست؟ VPN

بگویید: VPN یا شبکه خصوصی مجازی کامپیوتر شما را به سرور دیگری متصل می‌کند سپس از طریق آن به اینترنت دسترسی پیدا می‌کند، فعالیت شما را پنهان می‌کند. همچنین گاهی اوقات می‌تواند مکان شما را جعل کند و به شما امکان می‌دهد موانع جغرافیایی را دور بزنید.

توجه داشته باشید که یک VPN شما را در برابر قطع اینترنت محافظت نمی‌کند، زیرا IP شما در طول قطع اینترنت همچنان "فعال" است و تلاش می‌کند به VPN دسترسی پیدا کند، و این شما را آسیب‌پذیر می‌سازد!
VPNهای خوب شامل NordVPN یا Mullvad می‌باشند، اما به طور کلی اگر شما می‌خواهید یک VPN انتخاب کنید که لاگ‌ها را ذخیره نکند، زیرا در غیر این صورت، این اطلاعات به جای سرویس‌دهنده اینترنت شما به ارائه‌دهنده VPN منتقل می‌شود که سپس می‌تواند این داده‌ها را بفروشد یا از آن سوءاستفاده کند.

ب) مرورگرهای وب

بپرسید: از چه مرورگرهای وبی استفاده می‌کنید؟

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Brave? Vivaldi?

به طور کلی، خوب است که دو مرورگر وب داشته باشید: یکی که حساب‌های شما را دارد و برای کارهای حرفه‌ای یا شخصی همگام‌سازی شده است و دیگری فقط برای جستجوی ساده استفاده می‌شود. این به این دلیل است که موتورهای جستجو تاریخچه جستجوی شما را دنبال کرده و تجربه مرور شما را تغییر می‌دهند.

Mozilla Firefox و Vivaldi به طور کلی مرورگرهای امنی هستند. Chrome و MS Edge توسط توسعه‌دهندگان بزرگ نرم‌افزاری طراحی شده‌اند که می‌خواهند داده‌های شما را جمع‌آوری کرده و برای اهداف تجاری استفاده کنند. شما می‌توانید از unGoogled Chromium که منبع باز است و تمام ابزارهای استخراج داده گوگل را حذف کرده، استفاده کنید. Brave نیز دارای برخی تحلیل‌های داخلی است اما ویژگی‌های امنیتی بسیار قوی دارد. مرورگرهای کاملاً ناامن برای فعالان حقوق بشر شامل Opera (که داده‌هایش مستقیماً به یک سرور چینی می‌رود) و همچنین مرورگرهای داخلی که توسط شرکت‌های تبلیغاتی طراحی شده‌اند، می‌باشد.

قسمت 5: محافظت از شما در برابر فیشینگ و بدافزار

فیشینگ: "روش تقلبی ارسال ایمیل‌ها یا پیام‌های دیگر که ادعا می‌کنند از شرکت‌های معتبر هستند تا افراد را وادار کنند اطلاعات شخصی خود مانند رمزهای عبور و شماره‌های کارت اعتباری را فاش کنند " .

بدافزار: "نرم‌افزاری که به‌طور خاص برای مختل کردن، آسیب رساندن یا دسترسی غیرمجاز به سیستم کامپیوتری طراحی شده است " .

حملات فیشینگ اغلب با ایمیل‌ها مرتبط هستند، اما در واقع در تمام روش‌های ارتباطی دیگر نیز وجود دارند.ایده فیشینگ این است که شما به عنوان یک شخص مورد اعتماد طعمه‌ای را ارائه دهید. شاید درباره فیشینگ شنیده باشید

امروزه بسیاری از فیشینگ‌ها از طریق ایمیل انجام می‌شوند، اما ممکن است درباره کت‌فیشینگ، استفاده از برنامه‌های دوستیابی نیز شنیده باشید. در گذشته، شما کلاهبردارانی داشتید که از طریق تلفن با مردم تماس می‌گرفتند. یک هکری که از فیشینگ استفاده می‌کند، کسی است که در حال انجام مهندسی اجتماعی است، و هر چه بهتر در

مهندسی اجتماعی باشد، می‌تواند به شما آسیب بیشتری برساند

بیایید نگاهی به برخی پیام‌ها بیاندازیم که حاوی لینک‌هایی هستند که می‌توانند فیشینگ باشند:

اسلایدهایی با مثال‌ها را نمایش دهید و بپرسید چگونه می‌توان آنها را شناسایی کرد.

بگویید: ایده این است که اگر به لینکی مانند این برخورد کردید، باید بتوانید محیطی ایجاد کنید که کلیک بر روی آن و دانلود آن هرگونه بدافزار احتمالی را منزوی کند. این به عنوان سندباکسینگ شناخته می‌شود و یک مفهوم حیاتی در امنیت سایبری است. روش قدیمی سندباکسینگ این بود که یک کامپیوتر آفلاین داشته باشید، روی آن کار کنید و اطمینان حاصل کنید که هیچ توانایی اتصال به اینترنت ندارد. با این حال، به طور فزاینده‌ای می‌توانید با ایجاد یک ماشین مجازی سندباکسینگ کنید

یک ماشین مجازی مانند یکی از آن عروسک‌های روسی است که خود را باز می‌کند: یک سیستم عامل را درون یک سیستم عامل ایجاد می‌کند .

در نهایت، اگر شما به خصوص آسیب‌پذیر هستید و مرتباً تعداد زیادی بدافزار احتمالی از ایمیل، وب‌سایت‌ها یا سرویس پیام‌رسانی خود دریافت می‌کنید و واقعاً به امنیت سایبری علاقه‌مند هستید، به سیستم‌های عامل که از سندباکسینگ به عنوان یک اصل استفاده می‌کنند نگاه کنید.
مثالی از این سیستم‌ها QubesOS است که به شما امکان می‌دهد "محیط‌های" مختلفی ایجاد کنید که قادر به برقراری ارتباط با یکدیگر نیستند.

بخش ۶: اطمینان از امنیت ارتباطات شما

سوال: چرا سیستم پیامک در کشوری مانند ایران امن نیست؟

پاسخ:
سرویس‌های موبایل و ارائه‌دهندگان خدمات اینترنت در حکومت‌های دیکتاتوری اغلب داده‌های ورودی و خروجی تلفن شما را از طریق خدماتی مانند پیامک متمرکز می‌کنند. به همین دلیل استفاده از رمزگذاری انتها به انتها (End-to-End Encryption یا E2EE) بسیار مهم است .

رمزگذاری انتها به انتها یا E2EE یک روش امنیتی است که چت‌ها و پیام‌های شما را ایمن نگه می‌دارد. این ایده بر این اساس است که دو یا چند نفر یک کلید عمومی و یک کلید خصوصی دارند.

کلید عمومی در دسترس هر کسی که آن را درخواست کند قرار می‌گیرد و کلید خصوصی شما کلیدهای عمومی دیگران را رمزگشایی می‌کند. برای درک بهتر رمزگذاری انتها به انتها، در اینجا یک ویدئوی آموزشی مفید وجود دارد.

<نمایش ویدیو>

بگو:

حالا فرض می‌کنم همه شما از ایمیل استفاده می‌کنید و در مقایسه با واتس‌اپ، اینستاگرام، اسنپ‌چت و دیگر اپلیکیشن‌های پیام‌رسان ایمن‌تر که بررسی کرده‌ایم، فناوری ایمیل نسبتاً قدیمی است. به همین دلیل است که ضروری است بدانید از کدام ارائه‌دهنده ایمیل استفاده کنید، چه نوع تهدیداتی وجود دارد و کجا باید به دنبال منابع اضافی باشید.

حساب‌های ایمیل از دامنه‌هایی مانند gmail.com@ استفاده می‌کنند تا نشان دهند که از کدام سرورها برای انتقال پیام از طریق اینترنت استفاده می‌کنید. اغلب ایمیل کاری شما از سرورهای کاریتان استفاده می‌کند و دامنه organisationname.com@ دارد. بیشتر حساب‌های ایمیل توسط ارائه‌دهندگان خدمات ایمیل مانند گوگل یا مایکروسافت مدیریت می‌شوند.

یکی از تهدیدات کلیدی علاوه بر فیشینگ، جعل دامنه است .

جعل دامنه تلاش می‌کند از دامنه و هویت شما به عنوان یک سازمان یا حتی فرد برای سرقت ایمیل شما یا به دست آوردن اطلاعات با جلب‌توجه به عنوان شما استفاده کند. برای مقابله با جعل دامنه باید گزارش دهید .

رمزگذاری انتها به انتها در ایمیل نیز یک ابزار مفید است هنگام تبادل اطلاعات یا فایل حساس. ارائه‌دهندگان ایمیلی مانند جیمیل و اوتلوک به طور پیش‌فرض با رمزگذاری انتها به انتها همراه نیستند. اما برای جیمیل افزونه‌ای به نام Mailvelope وجود دارد که می‌تواند رمزگذاری کند. ارائه‌دهندگان ایمیل که از رمزگذاری انتها به انتها استفاده می‌کنند و حتی ابزارهایی دارند که فقط گیرنده می‌تواند پیام را رمزگشایی کند حتی اگر کلید عمومی شما را نداشته باشد، شامل Protonmail و Tutanota هستند. اما عیب این است که این‌ها تمایل به مشکلات سازگاری با کلاینت‌های ایمیل دارند و محیط‌های بسته‌ای با ویژگی‌های بسیار اولیه در مقایسه با جیمیل و اوتلوک دارند، اما برای استفاده تخصصی قطعا ارزش بررسی دارند.

بخش ۷: امنیت گوشی‌های هوشمند

سوال: نظرسنجی سریع از کسانی که از کدام سیستم‌عامل گوشی استفاده می‌کنند
(یا اندروید iOS)

بگو:
ما به طور مختصر درباره اپلیکیشن‌های پیام‌رسان در گوشی شما صحبت کرده‌ایم، اما ظهور گوشی‌های هوشمند چالش‌های متعددی را برای کارشناسان امنیت سایبری به همراه داشته است. یکی این است که تقریباً تمام زندگی شما اکنون می‌تواند در گوشی شما یافت شود، و همان‌طور که در ابتدای کلاس توضیح دادیم.

اسلاید اکس را نمایش دهید

بگو:
رسوایی پگاسوس نشان داد که حتی دولت‌های دموکراتیک آماده جاسوسی از شهروندان هستند و این کار را با استفاده از روش‌های فیشینگ که در بالا دیده‌ایم (برای مثال از طریق پیامک) انجام دادند. بسیاری از شما ممکن است قبلاً فکر کرده باشید که NSA، GCHQ و دیگر شرکت‌های اطلاعاتی سیگنال در حال جاسوسی از شما هستند. اما واقعیت این است که قبل از پگاسوس این گروه‌ها واقعاً فقط می‌توانستند ارتباطات شما بین شما و شخص ثالثی را بخوانند. دنیای پس از پگاسوس ترسناک است زیرا اکنون تمام گوشی شما می‌تواند تحت نظر قرار بگیرد و به همین دلیل هر هکر ماهری می‌تواند به طور بالقوه از ابزاری استفاده کند تا به اندازه کافی اطلاعات درباره شما به دست آورد تا شما را در برابر تهدیدها آسیب‌پذیر کند.

انتشار بدافزار هایی مانند پگاسوس به هکرها دسترسی به تمام گوشی شما را می‌دهد که این امر به ویژه غیرقانونی است. اما مهمتر از همه این نشان می‌دهد که گوشی‌های ما به راحتی به یک دستگاه نظارت قابل حمل تبدیل می‌شوند. و می‌توانید به این واقعیت اضافه کنید که گوگل، اپل و دیگر خدمات موبایل داده‌هایی را از شما جمع‌آوری می‌کنند برای اهداف تجاری که سپس می‌تواند در صورت افتادن به دست افراد نادرست علیه شما استفاده شود.

خوشبختانه، مجموعه‌ای از گزینه‌های جایگزین برای کسانی که نمی‌خواهند در استفاده از گوشی هوشمند آسیب‌پذیر باشند وجود دارد. Graphene OS و Lineage OS نمونه‌هایی از آنچه ما به عنوان شاخه‌های کد اندروید می‌نامیم هستند که تمام خدمات مرتبط با گوگل را حذف کرده‌اند. همچنین می‌توانید به سیستم‌عامل‌های گوشی نگاه کنید که می‌توانند به طور مؤثری از سندباکسینگ استفاده کنند تا مطمئن شوند که هیچ برنامه‌ای که نصب می‌کنید دیگران

را جاسوسی نمی‌کند.

اما توجه داشته باشید که به طور کلی گوشی شما ابزار ایده‌آل برای جاسوسی از شما است. از درایورهای سخت‌افزاری تا اپلیکیشن‌های بازی که دانلود می‌کنید، بیشتر فناوری موجود در گوشی شما بسته است: شما نمی‌دانید چه کدی توسعه‌دهنده بر روی گوشی شما قرار داده است. همان‌طور که ما به محیطی دیجیتالی بیشتر تحت‌سلطه گوشی‌های هوشمند و تبلت‌ها می‌رویم، بهترین شرط شما به عنوان یک فعال حقوق بشر استفاده کمترین از این ابزارها یا با نرم‌افزارهای بسیار تخصصی است.

بخش ۸: چند نکته نهایی و سوالات متداول

بگو: بیایید به چند سوال متداول بپردازیم که شاید برخی از شما بتوانید به آن‌ها کمک کنید پاسخ دهید، و سپس یک کارگاه کوچک برگزار کنیم که در آن شما از من سوال بپرسید

سوال: آیا باید یک ضد ویروس نصب کنم؟ اگر بله، کدام یک؟

پاسخ:
ضدویروس‌ها اغلب اکنون به سیستم‌عامل‌ها متصل هستند. روزهایی گذشته است که ویندوز برای مقابله با بدافزار به ارائه‌دهندگان ضدویروس شخص ثالث وابسته بود. اپل و لینوکس تمایل به قوی بودن در برابر بدافزار دارند، دومی به دلیل فلسفه منبع باز آن. به یاد داشته باشید که منبع باز به این معنی است که کد برای همه باز است و معمولاً توسط دیگر کدنویسان بررسی می‌شود تا صحت آن تایید شود.
با این حال، اگر یک ضدویروس نصب کرده‌اید یا می‌خواهید یکی بخرید، ضدویروس‌ها به طور کلی ابزارهای تجزیه و تحلیل داده‌ای هستند که نظارت می‌کنند کامپیوتر شما چگونه منابع خود را استفاده می‌کند، چه فایل‌هایی مشکوک یا خراب به نظر می‌رسند و همچنین می‌تواند به شما کمک کند فایروال خود را تقویت کنید - دیواری که مانع ورود بازیگران بد به شبکه/IP آدرس شما می‌شود. یک ضد ویروس خوب Bitdefender است، اما اگر یاد بگیرید که از سندباکسینگ استفاده کنید و از سیاست‌های ضدویروس عقلانی استفاده کنید، به آن نیازی نخواهید داشت.

سوال: آیا اپل واقعاً امن‌تر از ویندوز است؟

پاسخ: بله، اما همچنان در معرض آسیب‌پذیری‌ها قرار دارد. انتخاب سیستم‌عامل مناسب برای نوع کاری که انجام

می‌دهید نیز ضروری است. سیستم‌عامل‌های لینوکس رایگان بسیاری وجود دارد که در مقایسه با محصولات اپل و مایکروسافت بسیار امن‌تر و امن‌تر در نظر گرفته می‌شوند، اما ممکن است نیاز به تسلط فنی بیشتری داشته باشند. اما اگر می‌خواهید وارد امنیت سایبری شوید، یادگیری نحوه کار سیستم‌عامل‌های لینوکس، هک اخلاقی از طریق Kali Linux و تفاوت‌های اصلی در سیستم‌عامل‌ها برای استفاده‌های سروری و شخصی ضروری است.

پرسش: از کجا می‌توانم شروع کنم اگر می‌خواهم به عمق بیشتری در زمینه امنیت سایبری بروم؟

پاسخ: همان‌طور که قبلاً گفته شد، حوزه‌های زیادی وجود دارد که می‌توانید در زمینه امنیت سایبری وارد شوید. یک شروع خوب یادگیری اصول سخت‌افزار و برنامه‌نویسی نرم‌افزار است تا حداقل در رابطه بین این دو سواد داشته باشید و سپس یاد بگیرید که چگونه سرور خود را تنظیم کنید.

پرسش: چگونه بفهمم که کامپیوتر یا تلفنم هک شده است؟

پاسخ: همان‌طور که قبلاً گفته شد، شما معمولاً متوجه نمی‌شوید که هک شده‌اید تا زمانی که خیلی دیر شده باشد، زیرا هکرها تمایل دارند در پس‌زمینه سیستم‌عامل شما فعالیت کنند (دسترسی به فایل‌ها بدون اینکه شما متوجه شوید).

نکته:

- برای کامپیوتر، می‌توانید فایل‌های مشکوک را با استفاده از وب‌سایت‌های زیر بررسی کنید:
- برای تلفن‌ها، ابزارهای خوبی وجود دارد که می‌توانید بررسی کنید آیا به جاسوس‌افزار یا بدافزار آلوده شده‌اید:
- برای حساب‌های خاص، می‌توانید بررسی کنید که آیا دچار نشت داده یا هک شده‌اید از طریق این وب‌سایت:
- برای ایمیل یا وب‌سایت شخصی خود به خصوص، می‌توانید بررسی کنید که آیا دامنه شما تقلبی شده است یا نه از طریق بررسی دامنه:

پرسش: چه منابعی وجود دارد اگر به عنوان یک فعال حقوق بشر نیاز به کمک داشته باشم؟

پاسخ:

• AccessNow
• Amnesty Tech
• Center for Digital Resilience
• UNPO

سپس کارگاهی با موارد فردی بیشتر بر اساس مخاطبان و دستگاه‌هایی که در اختیار دارند برگزار کنید.