Ouch! ژانویه 2024

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

کدهای QR

مقدمه

آیا تا به حال فکر کرده اید که آن مربع های نقطه دار یا نوارهایی که "کدهای QR" نام دارند به چه کار می آیند؟ به احتمال زیاد آنها را در وب سایت ها، چاپ شده روی پوسترها، استفاده شده به عنوان بلیط های موبایل یا روی میزهای رستوران دیده اید. اینها چگونه کار می کنند و آیا خطراتی وجود دارد که باید نگران آنها باشید؟ بیایید دریابیم

کد QR که به وب سایت SANS OUCH اشاره می کند.

کدهای QR چگونه کار می کنند؟

کد QR مخفف "کد پاسخ سریع" است و یک کد قابل خواندن توسط ماشین است که معمولاً از ماتریسی شامل مربع‌های سیاه و سفید تشکیل شده است (همچنین می‌توانند در رنگ‌های دیگر و حاوی تصاویر پس‌زمینه باشند). این مربع ها را می توان به راحتی با تولیدکنندگان کد QR ایجاد کرد و میتوان از آنها برای رمزگذاری اطلاعاتی مانند URL های وب سایت، اطلاعات تماس ایمیل یا انواع دیگر داده ها استفاده کرد. به کدهای QR مانند بارکدها اما تطبیق پذیرتر بیاندیشید. اکثر دوربین های دستگاه های تلفن همراه، اطلاعات کد شده در یک کد QR را شناسایی و رمزگشایی می کنند. به عبارت دیگر، وقتی سعی می‌کنید از یک کد QR با دوربین دستگاه خود عکس بگیرید، کد QR را رمزگشایی می‌کند و از شما می‌پرسد که آیا می‌خواهید بر اساس اطلاعات موجود در آن عمل کنید، مانند باز کردن پیوند به یک وب سایت.

خطرات آن چیست؟

تفسیر آسان کدهای QR برای افراد دشوار است، که این امر باعث می‌شود مهاجمان سایبری بتوانند اطلاعاتی را که می‌توانند مخرب یا آسیب‌رسان باشند، رمزگذاری کنند. برای مثال، یک کد QR می‌تواند شما را به یک وب‌سایت مخرب بفرستد که تلاش می‌کند اطلاعات شخصی شما، مانند گذرواژه‌ها یا شماره‌های کارت اعتباری را جمع‌آوری کند، یا شاید حتی سعی کند بدافزار را روی دستگاه شما نصب کند. علاوه بر این، کدهای QR می‌توانند مراحل دیگری مانند افزودن یک مخاطب به فهرست مخاطبین یا نوشتن ایمیل را از طرف شما انجام دهند. کد QR به خودی خود یک تهدید نیست، با این حال، اطلاعات یا اقدامی که باعث می شود، می تواند شامل خطراتی باشد.

برای مثال، فرض کنید در شهر یا شاید در یک فرودگاه هستید، و پوستری روی دیواری وجود دارد و محصولی را که توجه شما را جلب کرده است تبلیغ میکند. پوستر دارای یک کد QR است که می توانید از آن برای دریافت سریع اطلاعات بیشتر استفاده کنید. چیزی که متوجه نمی‌شوید این است که شخصی، کد QR پوستر را با برچسبی از کد QR متفاوت پوشانده است. وقتی به پوستر نگاه می کنید به آن اعتماد می کنید، اما متوجه نمی شوید که کد QR روی پوستر توسط یک مجرم جایگزین شده است. وقتی کد QR را اسکن می‌کنید تا درباره محصول بیشتر بدانید، به وب‌سایتی که توسط مجرم کنترل می‌شود هدایت می‌شوید تا مهاجم بتواند حمله را شروع کند.

برای ایمن بودن چه باید بکنم؟

- قبل از اعتماد کردن و اسکن کردن کد QR مراقب باشید. ابتدا، از خود بپرسید: آیا میتوانید به منبع اعتماد کنید؟ آیا به پوستر، رستوران یا وب‌سایتی که کد QR را نشان می‌دهد اعتماد دارید؟ اگر کسی نوشته ای با کد QR روی ماشین شما گذاشت، آیا شما باورتان می شود؟
- هنگامی که یک کد QR را اسکن می‌کنید، دستگاه شما از شما می‌پرسد که آیا می‌خواهید قبل از انجام کاری بر اساس اطلاعاتی که می‌خواند عمل کنید. به عنوان مثال، اگر کد QR پیوندی به یک وب سایت باشد، دستگاه شما قبل از رفتن به سایت از شما می پرسد که آیا می خواهید از آن سایت بازدید کنید یا خیر. زمانی را به بررسی درخواست اقدام (Call to Action) یا خود پیوند اختصاص دهید و اطمینان حاصل کنید که با مشاهده آن احساس راحتی می کنید.
- اطمینان حاصل کنید که دستگاه های تلفن همراه شما همیشه به روز هستند و آخرین نسخه سیستم عامل خود را اجرا می کنند. این تضمین می کند که دارای آخرین ویژگی های امنیتی است. ساده ترین راه برای انجام این کار این است که به روز رسانی خودکار را در دستگاه خود فعال کنید.
- برای رمزگشایی کدهای QR نیازی به نصب برنامه های موبایل خاصی نیست، باید بتوانید به سادگی از دوربین داخلی دستگاه خود استفاده کنید. اگر وب سایتی از شما می خواهد که یک برنامه تخصصی اسکن QR را دانلود کنید، به احتمال زیاد تقلبی یا جعلی است.
- قبل از ارائه اطلاعات محرمانه یا شخصی به هر وب سایتی که از طریق یک کد QR قابل مشاهده برای عموم، به آن دسترسی پیدا کرده اید، دوباره فکر کنید.

کدهای QR راهی مناسب برای دسترسی به انواع اطلاعات و قابلیت های جدید هستند. انجام چند مرحله ساده می تواند به شما کمک کند تا بهترین استفاده را از آنها، ایمن و ایمن ببرید.

سردبیر مهمان

عبدالمجید ال عبدالهادی مشاور سیستم های IT/OT در عربستان سعودی آرامکو با بیش از 27 سال تجربه است. او یک حسابرس گواهی شده سیستم های اطلاعاتی (CISA) و مدیر خبره امنیت اطلاعات (CISM) با حق اختراع امنیت سایبری توسط اداره ثبت اختراع ایالات متحده (10,693,906) است.

منابع

Smishing/حملات پیام رسانی: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Vishing-حملات تماس تلفنی و کلاهبرداری: https://www.sans.org/newsletters/ouch/vishing
اااستفاده ایمن از دستگاههای تلفن همراه: https://www.sans.org/newsletters/ouch/securing-mobile-devices

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو