چرا فیشینگ خطرناک است؟

مجموعه شرکت‌های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

فیشینگ؛ یکی از روش‌های رایج کلاهبرداری در دنیا

فیشینگ یکی از رایج‌ترین جرائم سایبری است که از طریق ایمیل، تلفن یا پیام متنی توسط هکرها ارسال می‌شود. هدف از ارسال این ایمیل‌ها این است که افراد را به ارائه داده‌های حساس مانند: مشخصات فردی، اطلاعات بانکی و رمزهای عبور فریب دهد. از این اطلاعات برای دسترسی به حساب‌های مهم استفاده می‌شود که ضررهای مالی بسیاری به همراه خواهد داشت. در این مقاله به انواع حملات فیشینگ نگاهی می اندازیم.

ویژگی‌های رایج ایمیل‌های فیشینگ

دروغ یا واقعیت؟: پیشنهادات پرسود و منحصر به فرد فیشینگ برای جلب توجه مردم طراحی می‌شوند. به عنوان مثال، بسیاری از این ایمیل‌ها می‌گویند که شما برنده آیفون، قرعه کشی یا یک جایزه بزرگ شده‌اید. برای در امان ماندن فقط کافی است که روی هیچ ایمیل مشکوکی کلیک نکنید.

احساس نیاز (Sense of Urgency): تکنیک مورد علاقه مجرمان سایبری این است که از کاربران می‌خواهند «فوری» کاری را انجام دهند؛ چرا که این پیشنهاد فوق العاده فقط برای مدت زمان محدودی قابل استفاده است. حتی به شما می‌گویند که فقط چند دقیقه فرصت دارید تا پاسخ دهید! وقتی با این نوع ایمیل‌ها مواجه می‌شوید بهتر است که به آن توجهی نکنید.

ممکن است گاهی اوقات ایمیلی دریافت کنید مبنی بر اینکه حساب شما به حالت تعلیق درآمده و باید هرچه سریع‌تر اطلاعات شخصی خود را به روز کنید. این در حالی است که بیشتر سازمان‌ها قبل از فسخ حساب کاربری افراد زمان کافی را در نظر می‌گیرند و هرگز از مشتریان درخواست نمی‌کنند که اطلاعات شخصی خود را از طریق اینترنت به روز رسانی کنند. اگر به این نوع ایمیل دریافتی شک داشتید، به جای کلیک کردن روی لینک موجود در ایمیل، مستقیما وبسایت منبع را مشاهده کنید.

هایپر لینک‌ها (Hyperlinks): لینک همیشه آن چیزی نیست که به نظر می‌رسد! نگه داشتن ماوس روی یک لینک مشخص، آدرس وبسایت واقعی را به شما نشان می‌دهد که با کلیک روی آن به صفحه‌ی مورد نظر هدایت خواهید شد.

اما موضوع اصلی همینجاست. ممکن است یک سایت محبوب و معروف با غلط املایی کاملا جزئی مانند: "www.bankofarnerica.com" باشد. در این مثال "r" و "n" به اشتباه جایگزین "m" شده اند. پس به آدرس سایت موردنظر دقت کنید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

پیوست‌ها (Attachments): اگر لینک را در ایمیلی مشاهده کردید که انتظارش را نداشتید یا منطقی نبود، روی آن کلیک نکنید. اغلب این لینک‌ها شامل فایل‌هایی مانند: باج افزار یا سایر ویروس‌ها هستند. تنها فایلی که همیشه می‌توان با اطمینان روی آن کلیک کرد، یک فایل txt است.

فرستنده غیر عادی (Unusual Sender): چه فرستنده ایمیل برای شما آشنا به نظر برسد و چه غریبه، اگر چیزی غیرعادی، غیرمنتظره و یا به طور کلی مشکوک مشاهده کردید، روی آن کلیک نکنید.

انواع حملات فیشینگ چیست؟

امروزه فیشینگ به چیزی فراتر از سرقت اطلاعات تبدیل شده است. حملات سایبری در انواع مختلفی اجرا می‌شوند و در واقع به نوع این کلاهبرداری بستگی دارد. انواع فیشینگ عبارتند از:

Spear phishing: این حمله ایمیلی را برای افراد خاص در یک سازمان ارسال می‌کند. این افراد معمولا از میان دارندگان حساب بانکی با امتیاز بالا انتخاب می‌شوند.

دستکاری پیوند (Link manipulation): این حملات به شکل ایمیل‌هایی هستند که یک لینک به سایت مخرب دارند. در بیشتر موارد این سایت شبیه به یک سایت رسمی است.

کلاهبرداری از مدیر عامل: این پیام‌ها عمدتا برای افرادی که در بخش مالی سازمان مشغول به کارند ارسال می‌شود. این ایمیل آن‌ها را فریب می‌دهد و باعث می‌شود تا تصور کنند مدیر عامل یا سایر مدیران اجرایی از آن‌ها درخواست انتقال پول دارند.

محتوای مخرب: برخی مهاجمان محتوایی را که حاوی لینک مخرب است در سایت هدف بارگذاری می‌کنند. این لینک کاربران را فریب می‌دهد تا روی لینک کلیک کنند و به یک وب‌سایت جعلی هدایت شوند.

بدافزار: ممکن است کاربران با کلیک روی یک لینک مخرب بدافزار را در دستگاه خود دانلود کنند.

Smishing: مهاجمان از طریق SMS کاربران را فریب می‌دهند تا از طریق تلفن‌های هوشمند خود به سایت‌های مخرب دسترسی پیدا کنند.

Vishing: مهاجمان از نرم‌افزار تغییر صدا استفاده می‌کنند تا پیامی را به مخاطبان هدف بفرستند. این صدا به آن‌ها می‌گوید که باید با شماره‌ای که مورد نظر مهاجمان است تماس بگیرند.

Wi-Fi Evil Twin: با جعل وای فای رایگان، مهاجمان کاربران را فریب می‌دهند تا به یک هات اسپات مخرب متصل شوند تا بتوانند سو استفاده‌های مدنظر خود را انجام دهند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

جلوگیری از حملات فیشینگ

اگرچه هکرها هر روز تکنیک‌های جدیدی را ارائه می‌کنند، اما کارهایی وجود دارد که می‌توانید برای محافظت از خود و سازمان‌تان انجام دهید:

برای محافظت در برابر ایمیل‌های اسپم، می‌توان از فیلترهای اسپم استفاده کرد. این فیلترها مبدا پیام، نرم افزار مورد استفاده برای ارسال پیام و ظاهر پیام را ارزیابی می‌کنند تا تشخیص دهند که آیا اسپم است یا خیر. گاهی اوقات ممکن است فیلترهای اسپم ایمیل‌های دریافتی از منابع قانونی را نیز مسدود کنند، بنابراین همیشه 100٪ دقیق نیست.

در مرحله بعد تنظیمات مرورگر باید تغییر کند تا از باز شدن وب سایت‌های جعلی جلوگیری شود. مرورگرها لیستی از وب‌سایت‌های جعلی را ذخیره می‌کنند و وقتی می‌خواهید به آن‌ها دسترسی پیدا کنید، آدرس مسدود می‌شود یا یک پیام هشدار روی صفحه نمایان می‌شود. مرورگر فقط باید به وب‌سایت‌های قابل اعتماد اجازه باز شدن را بدهد.

بسیاری از وب سایت‌ها از کاربران می‌خواهند که هنگام نمایش پروفایل کاربر، اطلاعات ورود را وارد کنند. این نوع سیستم ممکن است نوعی فیشینگ باشد. یکی از راه‌های تضمین امنیت این است که رمز عبور خود را به طور منظم تغییر دهید و هرگز از یک رمز عبور برای چندین حساب استفاده نکنید. همچنین، بهتر است وب‌سایت‌ها برای امنیت بیشتر از سیستم CAPTCHA استفاده کنند. بانک‌ها و سازمان‌های مالی از سیستم‌های نظارتی برای جلوگیری از کلاهبرداری استفاده می‌کنند.

افراد می‌توانند این کلاهبرداری را به سازمان‌های مرتبط گزارش دهند تا اقدامات قانونی علیه این وب سایت‌های کلاهبردار انجام شود. سازمان‌ها باید آموزش‌های آگاهی امنیتی را به کارکنان ارائه دهند تا خطرات احتمالی شناسایی شود.

برای جلوگیری از فیشینگ، عادات کاربران نیز باید تغییر کند. به عنوان مثال، همیشه قبل از وارد کردن مشخصات فردی خود بصورت آنلاین، شخصا با شرکت تماس بگیرید. یا اگر لینکی در ایمیل وجود دارد، ابتدا نشانگر را روی URL نگه دارید. وب‌سایت‌های ایمن با گواهینامه معتبر (SSL) با «https» شروع می‌شوند. در واقع همه سایت‌ها باید SSL معتبر داشته باشند.

در صورتی که اطلاعات شخصی خود را در مدت زمان طولانی به روز رسانی نکرده باشید، بانک هیچوقت اطلاعات شخصی رشما را از طریق ایمیل درخواست نمی‌کند! اغلب بانک‌ها و موسسات مالی معمولا شماره حساب را در ایمیل ارائه می‌کنند یک منبع قابل اعتماد است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

فیشینگ چه صنایعی را هدف قرار می‌دهد؟

در اکثر موارد هدف فیشینگ سود مالی است، بنابراین مهاجمان عمدتا صنایع خاصی را هدف قرار می‌دهند. این هدف می‌تواند کل سازمان یا تک تک کاربران آن باشد. صنایعی که بیشتر در معرض خطر هستند، عبارتند از:

- فروشگاه‌های آنلاین (تجارت الکترونیک)
- رسانه‌های اجتماعی
- بانک‌ها و سایر موسسات مالی
- سیستم‌های پرداخت (پردازنده‌های کارت بازرگانی)
- شرکت‌های فناوری اطلاعات
- شرکت‌های مخابراتی
- شرکت‌های پستی
- برندهای تقلبی

هکرها از مارک‌های معروف برای فریب افراد استفاده می‌کنند. مارک‌های معروف اعتماد گیرندگان را تحریک می‌کنند و شانس موفقیت آمیز بودن حمله را افزایش می‌دهند. هر برند مشهوری را می‌توان در کلاهبرداری استفاده کرد، اما چند مورد رایج عبارتند از:

- گوگل
- مایکروسافت
- آمازون
- ولز فارگو
- بانک آمریکا
- Apple
- لینکدین
- فدرال اکسپرس

آمار فیشینگ

فیشینگ یک تهدید بزرگ برای افراد و مشاغل است. آمار زیر کمی از جدی بودن این حملات را نشان می‌دهد:

- 241,324 حملات در سال 2020 گزارش شد که 110 درصد افزایش نسبت به سال 2019 داشته است.
- 75% از پاسخ دهندگان نظرسنجی قربانی این حملات شده‌اند.
- 96% حملات با استفاده از ایمیل انجام می‌شود.
- میانگین هزینه برای یک سازمان قربانی این کلاهبرداری 3.92 میلیون دلار است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

مشکلات مخرب فیشینگ در زندگی افراد مختلف

تشخیص عواقب حمله فیشینگ چه در خانه و چه در محل کار بسیار مهم است. در اینجا به چند مورد از مشکلاتی است که ممکن است این نوع کلاهبرداری برای شما ایجاد کند، اشاره می‌کنیم.

زندگی شخصی

- سرقت پول از حساب‌های بانکی
- هزینه‌های جعلی از کارت اعتباری
- تنظیم اظهارنامه مالیاتی که به نام شخص مورد نظر
- افتتاح وام‌هایی که به نام شخص
- از دست دادن دسترسی به عکس‌ها، فیلم‌ها، فایل‌ها و سایر اسناد مهم.
- انتشار پست‌های جعلی در شبکه‌های اجتماعی در حساب اشخاص

محل کار

- از دست دادن وجه سازمان
- افشای اطلاعات شخصی مشتریان و همکاران
- دسترسی افراد خارجی به فایل‌ها و سیستم‌های محرمانه
- قفل و غیر قابل دسترس شدن فایل‌ها
- آسیب به شهرت کارفرما
- جریمه‌های مالی
- از دست رفتن ارزش شرکت
- کاهش اعتماد سرمایه گذاران
- وقفه در بهره وری تاثیرگذار بر درآمد

نتیجه گیری

مجرمان سایبری از ایمیل‌های اسپم استفاده می‌کنند زیرا آسان، ارزان و موثر است. در واقع هکرها با کمترین تلاش و هزینه می‌توانند به سرعت به داده‌های ارزشمند دسترسی پیدا کنند. داده‌هایی که مجرمان سایبری به دنبال آن هستند شامل مشخصات شخصی مانند: اطلاعات حساب مالی، شماره کارت اعتباری و سوابق مالیاتی و پزشکی و همچنین اطلاعات تجاری حساس مانند: نام مشتریان و اطلاعات تماس و ارتباطات محرمانه است.

با رعایت نکات و توصیه‌های ساده ای که در این مقاله گفتیم و استفاده از ابزارهای مناسب پیشگیری از فیشینگ می‌توانید خطر قربانی شدن در برابر کلاهبرداران دیجیتال را تا حد زیادی به حداقل برسانید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net