سرقت هویت و مقابله با آن

حمله های phishingیا سرقت هویت چیزی فراتر از هرزنامه های ناخواسته و مزاحم هستند. آنها می توانند منجر به دزدیده شدن شماره های اعتباری، کلمات عبور، اطلاعات حساب یا سایر اطلاعات شخصی کاربر شوند. این حمله ها در واقع نوعی از حملات مهندسی اجتماعی هستند که با استفاده از فریب کاربران سعی در به دست آوردن اطلاعات محرمانه از آنها دارند .

- **یک حمله مهندسی اجتماعی چیست؟**

برای انجام یک حمله مهندسی اجتماعی، مهاجم به تعامل با کاربر برای به دست آوردن اطلاعات در مورد سازمانها و یا سیستم های کامپیوتری نیاز دارد. فرد مهاجم معمولاً بسیار ساده و قابل احترام به نظر می رسد و ممکن است ادعا کند کارمند جدید، تعمیرکار و یا محقق است. حتی گاهی اوقات تاییدیه ای را به فرد قربانی نشان می دهد و ادعا می کند که برای پشتیبانی از وی فرستاده شده است. به هر حال با پرسیدن سؤالات، فرد مهاجم می تواند اطلاعات خرد به دست آمده را کنار هم گذاشته و به اطلاعات کافی برای شکستن سد دفاعی شبکه یک سازمان دست پیدا کند. این افراد معمولاً با به دست آوردن اطلاعات کمی از فردی در سازمان مورد نظر، بنا بر اطلاعات به دست آمده سعی می کنند تا با پرسیدن سؤالات تخصصی تر از افراد دیگر در همان سازمان، دامنه اطلاعات خود را گسترش دهند .

- **منظور از حمله سرقت هویت چیست؟**

همان طور که گفته شد، حملات سرقت هویت نوعی از حملات مهندسی اجتماعی هستند. حملات سرقت هویت از ایمیلها یا وب سایتهای خرابکاری که ظاهرا به یک سازمان قابل اطمینان تعلق دارند، برای به دست آوردن اطلاعات از افراد سوءاستفاده می کنند. برای مثال، فرد مهاجم یک ایمیل را برای فرد قربانی ارسال می کند که به نظر می رسد از یک شرکت صاحب کارت اعتباری و یا از یک مؤسسه مالی ارسال شده است و در آن از کاربر خواسته می شود اطلاعات حساب کاربری خود را به علت به وجود آمدن یک مشکل وارد کند. زمانی که کاربر اطلاعات خواسته شده را به خیال معتبر بودن ایمیل برای فرستنده ارسال می کند، مهاجم قادر است با استفاده از اطلاعات مذکور به حساب کاربری فرد قربانی دسترسی پیدا کند. حملات سرقت هویت می توانند از طریق دیگر مؤسسات نیز انجام شوند که اغلب مؤسسات خیریه می باشند و از وقایع روز یا مناسبتهای موجود در سال برای فریب کاربران استفاده می کنند. برای مثال می توان به مصائب طبیعی (سونامی اندونزی)، ترس از اپیدمی بیماریها(H۱N۱) ، مسائل اقتصادی، انتخابات ها و تعطیلات اشاره کرد .

در زیر چندین راهکار برای اجتناب از قربانی شدن در حملات سرقت هویت آورده شده است :

- **تغییر منظم رمز عبور**

متخصصان امنیتی پیشنهاد می کنند، کاربران هر سه ماه یک بار رمز عبور حسابهای کاربری خویش را تغییر دهند. در ضمن بهتر است که از رمز عبورهای یکسان در وب سایتهای مختلف استفاده نشود. تغییر منظم رمزهای عبور مختلف بر روی وب سایتهای گوناگون و به خاطر سپردن همه آنها کار چندان ساده ای نیست. برای این منظور بهتر است از نرم افزارهای مدیریت رمز عبور مانند LastPass یا RoboForm استفاده کرد که رمزهای عبور قوی را تولید و مدیریت می کنند .

- **کلیک با احتیاط**

در صورتی که کاربر ایمیلی را ظاهراً از یک وب سایت معتبر دریافت کند و در آن به هر دلیلی از وی خواسته شود تا بر روی لینکی کلیک کند، لازم است قبل از کلیک کردن لحظه ای تأمل کند. لینک مذکور ممکن است وی را به یک وب سایت تقلبی ارجاع دهد که قصد جمع آوری اطلاعات برای سرقت هویت یا دیگر جرائم اینترنتی را دارد. روش مطمئن تر تایپ URL صحیح در نوار آدرس است. در مورد وب سایتهایی که شماره ملی و یا شماره کارت اعتباری را درخواست می کنند باید بسیار مراقب بود و با احتیاط عمل کرد. همچنین کاربر باید از تطابق آدرس وب سایت با سایتی که در حال مشاهده آن است، اطمینان حاصل کند .

- **استفاده از وب سایتهای امن**

در صورتی که کاربر در حال ارسال اطلاعات کارت اعتباری و یا دیگر اطلاعات حساس به وب سایتی است، لازم است دقت کند که حتماً آدرس وب سایت مذکور با httpsشروع شود که s در اینجا نماینده security یا امنیت است. همچنین باید علامت قفل که معمولاً در قسمت پایین و سمت راست مرورگر مشاهده می شود، در وب سایت مذکور موجود باشد .

این نشانه دلالت بر استفاده وب سایت از رمزنگاری برای کمک به محافظت از اطلاعات حساس دارد. (شماره کارت اعتباری، شماره کارت ملی و جزئیات پرداخت که کاربر وارد می کند.) اگر کاربر بر روی این علامت دوبار کلیک کند، گواهی امنیتی سایت نشان داده می شود. نام بعد از Issued to باید با سایتی که کاربر در آن حضور دارد، مطابقت کند و در صورتی که نام متفاوت است، احتمالاً در سایت جعلی قرار دارد .

- **مرور منظم اعلامیه های کارت اعتباری و بانك**

حتی اگر کاربر سه مرحله قبل را به درستی انجام دهد، هنوز ممکن است قربانی دزدی هویت شود. در صورتی که کاربر اعلامیه های بانک و کارت اعتباری را حداقل ماهانه مرور کند، ممکن است بتواند یک جاعل را شناسایی و از وارد آمدن خسارات قابل توجه جلوگیری کند .

- **استفاده از فیلترهای ضد سرقت و نرم افزارهای مطمئن ضد بدافزار**

خوشبختانه امروزه در مرورگرهای جدید امکانات فیلتر کردن سایتهای سرقت هویت وجود دارد و بسته های نرم افزاری آنتی ویروس معروف نیز امکاناتی مشابه را ارائه می کنند. فایده دیگر نرم افزارهای ضد بدافزار مراقبت از کاربر در برابر سرقت ضربات صفحه کلید است. لازم است کاربران برای مقابله با حملات خرابکارانه آنتی ویروس خود را همواره به روز نگه دارند .

- **تفکر منتقدانه**

در صورتی که چیزی خوبتر از آن به نظر می رسد که حقیقت داشته باشد، در اغلب موارد واقعاً خوبتر از آن است که حقیقت داشته باشد. لازم است کاربران در مشاهده وب سایتهایی که وعده های باورنکردنی به آنها می دهند دقت لازم را به عمل آورند .

- **گزارش سو ءاستفاده های مشکوك از اطلاعات شخصی به مراکز مناسب**

قربانیان حملات سرقت هویت باید :

فوراً جعل را به شرکتی که جعل در مورد آن صورت گرفته است، گزارش کنند. اگر مطمئن نیستند که چگونه با شرکت تماس بگیرند، بهتر است وب سایت شرکت را برای گرفتن اطلاعات صحیح تماس، نگاه کنند. شرکت ممکن است یک آدرس ایمیل مخصوص برای گزارش چنین سو ءاستفاده ای داشته باشد. لازم است جزئیات جعل مانند ایمیل های دریافت شده، به مراکز ذیصلاح قانونی همچون مرکز ماهر نیز گزارش شود.

منبع : مرکز مدیریت امداد و هماهنگی ماهر