Ouch! سپتامبر 2024

صداهای اشباح: دفاع در برابر حملات شبیه سازی صدا

تماس غیرمنتظره: داستانی از فریب

مارگارت، یک معلم بازنشسته، از صبح های آرام خود در خانه کوچکش در حومه شهر لذت می برد. یک روز در حالی که او در حال لذت بردن از قهوه صبحگاهی خود بود، یک تماس دیوانه وار از نوه اش، جیکوب، که در کالج و دور از خانه بود، دریافت کرد. صدایش پر از وحشت شد و توضیح داد که تصادف کرده و برای پرداخت خسارت و جلوگیری از مشکلات قانونی نیاز فوری به پول دارد. اگر فوراً پول را دریافت نمی کرد، ممکن بود به زندان بیفتد. صدای آن طرف بی‌تردید صدای جیکوب بود - قلب مارگارت از نگرانی می‌تپید. او بدون سؤال به بانک خود رفت و به حسابی که جیکوب ارائه کرده بود پول ارسال کرد. مارگارت بعداً در همان روز با مادر جیکوب تماس گرفت تا از نحوه عملکرد جیکوب مطلع شود، همان موقع بود مارگارت متوجه شد که مورد کلاهبرداری قرار گرفته است. این تماس یک ترفند بی‌رحمانه بود، یک مجرم سایبری از فناوری شبیه‌سازی صدای هوش مصنوعی (AI) برای تقلید از صدای جیکوب استفاده کرده بود و از عشق و نگرانی مارگارت برای نوه‌اش سوء استفاده کرد.

شبیه سازی صدا چیست؟

شبیه سازی صدا زمانی است که شخصی از هوش مصنوعی برای بازآفرینی صدای یک فرد استفاده می کند تا الگوهای صوتی، لحن ها و ریتم های گفتار او را در بر بگیرد و یک کپی تقریباً عالی ایجاد کند.

حمله شبیه سازی صوتی با جمع آوری نمونه های صوتی از صدای هدف توسط یک مجرم سایبری آغاز می شود. این نمونه‌ها را می‌توان از منابع مختلفی مانند ویدیوهای YouTube یا پست‌های شخصی در TikTok جمع‌آوری کرد. پس از آموزش بر روی صدای ضبط شده، هوش مصنوعی صدای جدیدی تولید می کند که صدایی شبیه هدف دارد. این صدای تولید شده را می توان به روش های مختلفی استفاده کرد، از تماس های تلفنی گرفته تا پیام های صوتی، که آن را به ابزاری قدرتمند برای فریب تبدیل می کند.

هنگام ایجاد حملات شبیه سازی صوتی، اغلب مهاجمان سایبری ابتدا تحقیقات خود را انجام می دهند. بیشتر اطلاعات مورد نیاز آنها در سایت های رسانه های اجتماعی به صورت عمومی در دسترس است. آنها قربانیان مورد نظر خود را مورد مطالعه قرار می دهند تا هم صدای فردی را که قرار است تکرار کنند و هم قربانی را که قرار است با او تماس بگیرند را شامل شود. مجرمان سایبری نه تنها می آموزند که قربانیان آنها چه کسانی را می شناسند و به آنها اعتماد دارند، بلکه می آموزند که کدام محرک های عاطفی مؤثرترین هستند. هنگام برقراری این تماس‌های تلفنی، مهاجمان سایبری اغلب شناسه تماس‌گیرنده خود را تغییر می‌دهند، بنابراین وقتی قربانیان به تلفن‌هایشان نگاه می‌کنند، به نظر می‌رسد که تماس تلفنی از شماره‌ای است که قربانی به آن اعتماد دارد. شناسه تماس گیرنده را می توان به راحتی جعل کرد و راه خوبی برای تأیید اعتبار یا احراز هویت افرادی که با شما تماس می گیرند نیست.

از خودتان محافظت کنید

اولین قدم برای محافظت از خود این است که بدانید شبیه سازی صوتی اکنون امکان پذیر است و انجام آن برای مهاجمان سایبری آسان تر شده است. برخی از مراحل کلیدی که میتوانید برای حفاظت از خودتان انجام دهید عبارتند از:

- **حریم خصوصی**: از اطلاعاتی که با دیگران به اشتراک می گذارید آگاه باشید و آنها را محدود کنید و افرادی که می توانند به ضبط های شما در رسانه های اجتماعی دسترسی داشته باشند را محدود کنید.

- **سرنخ ها**: مراقب شاخص های رایجی باشید که نشان می دهد چیزی اشتباه است. هر زمان که شخصی با احساس فوریت شدید با شما تماس می گیرد یا شما را تحت فشار قرار می دهد که فوراً باید اقدام به کاری کنید، به احتمال زیاد کلاهبرداری است. هر چه احساس اضطرار بیشتر باشد، مانند مطالبه فوری پول، احتمال بیشتری وجود دارد که کسی سعی کند شما را با عجله به اشتباه بیاندازد. سایر شاخص‌های رایج عبارتند از چیزی که بیش از حد خوب است که درست باشد (نه شما در قرعه‌کشی برنده نشده‌اید) یا زمانی که تماس غیرمنتظره‌ای دریافت می‌کنید که به نظر عجیب می‌رسد.

- **تائیدش کنید**: اگر مطمئن نیستید که یک تماس تلفنی مشروع است، تماس را قطع کنید و با یک شماره تلفن مطمئن با فرد تماس بگیرید. به عنوان مثال، اگر از یک مدیر ارشد یا همکار در شرکت خود تماس تلفنی دریافت می کنید، با شماره تلفن مورد اعتمادی که می دانید واقعاً مال آنهاست، با آنها تماس بگیرید. اگر تماس تلفنی عجیبی از یکی از اعضای خانواده دریافت کردید، سعی کنید با او تماس بگیرید (شاید حتی از تماس ویدیویی استفاده کنید) یا با یکی دیگر از اعضای خانواده که آنها را به خوبی می شناسد تماس بگیرید.

- **رمز عبور**: یک رمز عبور یا رمز عبور مخفی ایجاد کنید که فقط شما و خانواده تان می دانید. به این ترتیب، اگر تماس تلفنی عجیبی دریافت کردید که به نظر می‌رسد از طرف یکی از اعضای خانواده باشد، می‌توانید با دیدن اینکه آیا رمز عبور مخفی شما را می‌دانند، تأیید کنید.

سردبیر مهمان

ماریا سینگ یک مدیر محتوای سایبری در EnterpriseKC و یکی از اعضای پرشور WiCyS با بیش از 14 سال تجربه در زمینه فناوری و امنیت سایبری است. او دارای گواهینامه SANS GIAC GSEC و کاندیدای کارشناسی ارشد علوم در امنیت سایبری در دانشگاه پردو است. ماریا به عنوان رئیس سابق زنان در امنیت کانزاس سیتی و دریافت کننده جایزه دستاوردهای شرکتی OCA، الهام بخش زنان در STEM و امنیت سایبری است. مشارکت های سخنرانی و رهبری او راه را برای نسل های آینده برای شکوفایی در این زمینه ها هموار می کند.

منابع

سه روشی که مهاجمان سایبری شما را هدف قرار می دهند: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
جلوی حملات تماس تلفنی فریبکارانه را بگیرید: https://www.sans.org/newsletters/ouch/stop-phone-call-scams
محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو