تحلیل امنیت (security)و حریم خصوصی (privacy)در اپلیکیشن‌های شناسایی تماس مطالعه موردی :

NumberBox و Truecaller

اداره کل حراست

استانداری چهارمحال و بختیاری

پاییز ۱۴۰۴

بسم الله الرحمن الرحیم

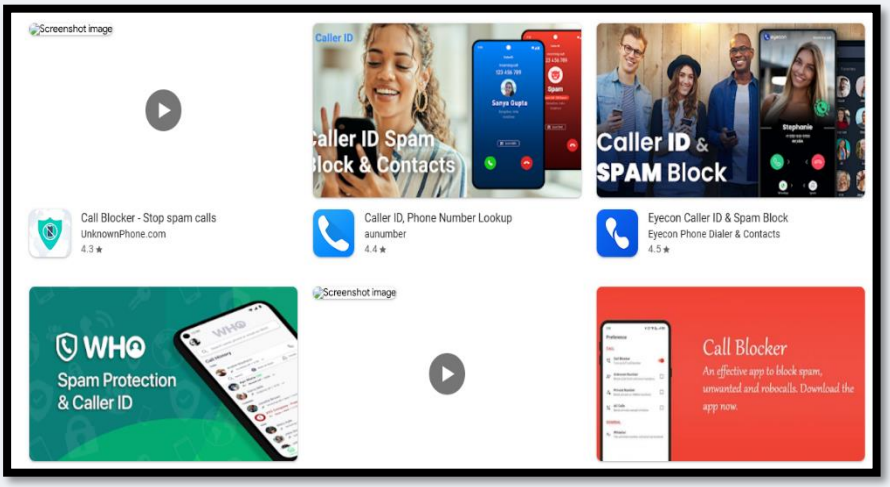
مقدمه

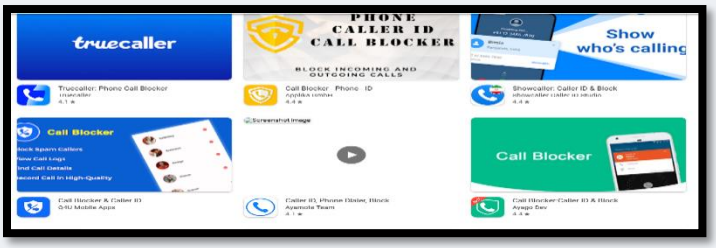
*با گسترش تلفن‌های هوشمند و افزایش تماس‌های ناخواسته و تبلیغاتی، اپلیکیشن‌هایی برای شناسایی تماس‌های ناشناس رواج یافته‌اند. این اپلیکیشن‌ها با دسترسی به پایگاه‌داده‌ای گسترده از شماره‌ها، امکان نمایش نام تماس‌گیرنده را حتی در صورت ذخیره نبودن در مخاطبین کاربر فراهم می‌سازند. با این حال، نحوه‌ی جمع‌آوری و استفاده از اطلاعات کاربران در این سامانه‌ها، پرسش‌های جدی در خصوص حریم خصوصی افراد ایجاد کرده است.*از جمله این اپلیکیشن ها می توان به موارد زیر اشاره کرد :

NumberBox ، Showcaller ، Hiya ، CallApp ، CIA - Caller ID & Call Blocker ، Truecaller و ...

ویژگی‌عملکردی این اپلیکشن ها شامل شناسایی شماره، مسدود کردن تماس، پیام‌رسانی، وضعیت آنلاین بودن، جستجوی معکوس شماره می باشد که برخی از آن ها در پلتفرم *IOS* و اندروید و برخی فقط بر روی اندروید نصب می گردند.

در این پژوهش با بررسی دو مورد از پرکاربردترین و محبوب ترین این دسته از اپلیکیشن ها یعنی Truecaller و NumberBox به بررسی امنیت و حریم خصوصی افراد می پردازیم.



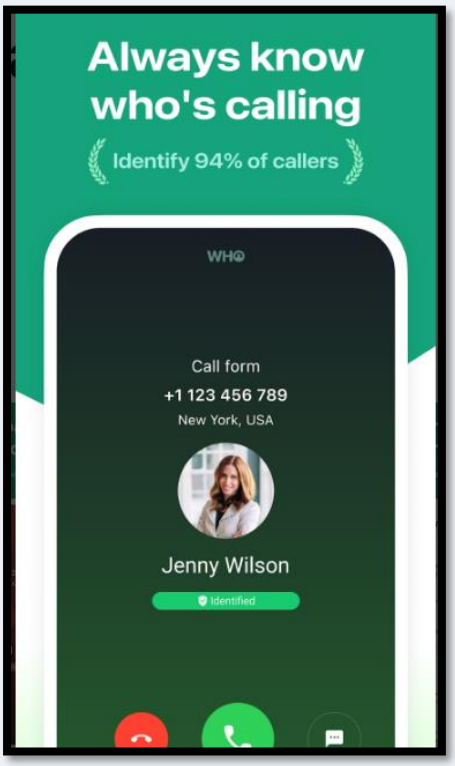


چکیده:

مدیران و مسئولان ارشد سازمانی و دولتی از جمله گروه‌هایی هستند که به دلیل حجم بالای تماس‌های ناشناس، نیاز بیشتری به ابزارهای هوشمند شناسایی تماس احساس می‌کنند. این نرم‌افزارها می‌توانند در غربال‌گری تماس‌های ضروری از مزاحم یا تبلیغاتی مؤثر باشند، اما در سطح مدیریتی و امنیتی، ریسک‌های قابل‌توجهی ایجاد می‌کنند.

از طرف دیگر الگوی بومیِ ذخیره‌سازی سبب می‌شود تا در صورت دسترسی نرم‌افزارها به فهرست مخاطبین، داده‌هایی فراتر از شماره تلفن گردآوری گردد؛ داده‌هایی که می‌تواند شبکه‌های ارتباطی، جایگاه شغلی و حتی روابط شخصی افراد را آشکار سازد.

جمع‌آوری داده بدون رضایت مستقیم افراد



یکی از اصلی‌ترین نقدهای وارد بر این اپلیکیشن‌ها، **جمع‌آوری اطلاعات اشخاصی است که خودشان هیچ‌گاه از اپلیکیشن استفاده نکرده‌اند** .به‌عنوان مثال، وقتی کاربری اپلیکیشن را نصب می‌کند و دسترسی به مخاطبین را می‌پذیرد، اطلاعات تماس افراد دیگر (نام، شماره و گاهی ایمیل) به سرور منتقل می‌شود. این اطلاعات سپس در نتایج جستجوی دیگر کاربران نمایش داده می‌شود.

در یک پژوهش انجام‌شده در دانشگاه آرهوس دانمارک (۲۰۲۱)، مشخص شد بیش از ۷۰٪ داده‌های موجود در دیتابیس *Truecaller* از طریق دسترسی به مخاطبین کاربران جمع‌آوری شده، نه ثبت‌نام مستقیم افراد.

پروفایل‌سازی خودکار و نمایش عمومی طلاعات

اپلیکیشن‌هایی مانند Truecaller با ترکیب اطلاعاتی از منابع مختلف، پروفایل‌هایی از شماره تلفن‌ها می‌سازند که ممکن است شامل:

- نام و نام خانوادگی
- عکس(مثلاً از حساب Gmail یا شبکه‌های اجتماعی)
- ایمیل
- محل کار یا منطقه جغرافیایی
- وضعیت "آنلاین بودن"

باشد. این اطلاعات حتی بدون رضایت صریح شخص در دسترس عموم قرار می‌گیرد .این پروفایل‌سازی خودکار می‌تواند باعث **نقض حریم خصوصی، ریسک‌های امنیتی و حتی سوءاستفاده‌های اجتماعی و تجاری** شود.

ذخیره‌سازی و پردازش داده‌ها در سرورهای خارجی

از آنجایی که بیشتر این اپلیکیشن‌ها توسط شرکت‌های خارجی توسعه یافته‌اند (مانند شرکت سوئدی *True Software Scandinavia AB*)داده‌های کاربران کشورهای مختلف، از جمله ایران، در سرورهای خارج از کشور ذخیره می‌شوند. این مسئله می‌تواند شامل **نقض حاکمیت داده *(data sovereignty)*** نیز باشد.

تضاد با قوانین بین‌المللی و داخلی

قانون(*GDPR* اتحادیه اروپا) به صراحت تأکید می‌کند که داده‌های افراد تنها با **رضایت آگاهانه** آن‌ها باید جمع‌آوری شود.اپ‌هایی مانند *Truecaller* به دلیل جمع‌آوری اطلاعات افراد غیرکاربر، با انتقاداتی در اروپا مواجه شده‌اند.

در ایران، اگرچه قانون جامع حفاظت از داده‌های شخصی هنوز تصویب نشده، اما بر اساس «قانون جرایم رایانه‌ای» و اصول «حقوق شهروندی در فضای مجازی»، جمع‌آوری بدون رضایت داده‌ها می‌تواند مصداق نقض حریم خصوصی باشد.

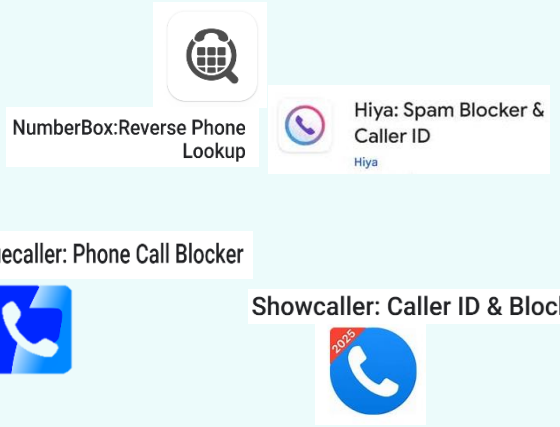
تجربه کاربران و نارضایتی عمومی

در سال‌های اخیر، کاربران زیادی در فروم‌ها، شبکه‌های اجتماعی و مارکت‌هایی مثل (*Google Play*)از این موضوع که شماره و نام‌شان بدون رضایت در *Truecaller* نمایش داده می‌شود، ابراز نگرانی کرده‌اند. حتی برخی افراد گزارش داده‌اند که اطلاعات‌شان به اشتباه با نام شخص دیگری نمایش داده شده است، که این خود منجر به مشکلاتی نظیر **سوءتفاهم‌های شغلی یا شخصی** شده است.

راهکارها و پیشنهادهای سیاست‌گذاری

برای کاهش مخاطرات حریم خصوصی، پیشنهادهای زیر ارائه می‌شود:

- **شفاف‌سازی سیاست‌های داده‌ای توسط توسعه‌دهندگان**:
  شرکت‌ها باید به‌صورت واضح توضیح دهند که چه داده‌هایی جمع‌آوری می‌شود و چگونه استفاده می‌شود.
- **اعمال محدودیت در دسترسی به مخاطبین**:
  لازم است دسترسی به مخاطبین، تنها با اطلاع کامل کاربر و برای اهداف مشخص انجام شود.
- **امکان حذف اطلاعات از دیتابیس *(opt-out)***
  اپلیکیشن‌ها باید امکان حذف کامل اطلاعات شخصی را برای هر فرد بدون نصب اپلیکیشن فراهم کنند.
- **ایجاد و اجرای قوانین داخلی حفاظت از داده‌ها در ایران:**
  تدوین قانون جامع حریم خصوصی دیجیتال می‌تواند به محافظت از حقوق کاربران ایرانی کمک کند .



ارتباط ساختاری بین نرم‌افزارهای HotVPN،NumberBox

در بررسی نرم‌افزارهای مشابه *Truecaller* ، نکته مهمی که می‌تواند به درک بهتر ساختار توسعه این برنامه‌ها کمک کند، شناسایی شرکت‌ها یا تیم‌های توسعه‌دهنده آنها است. بر اساس اطلاعات موجود در فروشگاه‌های رسمی اپلیکیشن‌ها، نرم‌افزارهای *NumberBox* و *HotVPN* هر دو تحت مالکیت و توسعه شرکت یا توسعه‌دهنده‌ای با نام *HotCodes* منتشر شده‌اند.

این امر نشان می‌دهد که این دو اپلیکیشن، اگرچه در حوزه‌های متفاوت فعالیت می‌کنند *NumberBox* در زمینه شناسایی شماره تماس و *HotVPN* در زمینه خدمات فیلترشکن و *VPN* اما از یک بستر توسعه مشترک برخوردار هستند. این موضوع می‌تواند به دلایل متعددی اهمیت داشته باشد:

- **یکپارچگی در سیاست‌های حفظ حریم خصوصی:**

با توجه به اینکه هر دو اپلیکیشن تحت یک توسعه‌دهنده هستند، احتمال اشتراک سیاست‌های داده و حریم خصوصی وجود دارد که می‌تواند تاثیر مستقیمی بر نگرانی‌های کاربران داشته باشد.

- **اشتراک فناوری و زیرساخت:**

استفاده از یک زیرساخت مشترک می‌تواند باعث بهبود امنیت و کیفیت خدمات شود، اما همچنین ممکن است ریسک‌هایی در زمینه نگهداری و مدیریت داده‌ها به همراه داشته باشد.

- **استراتژی‌های تجاری و بازاریابی:**

شرکت توسعه‌دهنده ممکن است از این دو اپلیکیشن برای پوشش بخش‌های مختلف بازار استفاده کند و داده‌ها یا کاربران را بین آن‌ها به اشتراک بگذارد.

با توجه به این ارتباط، تحلیل دقیق‌تر سیاست‌های حریم خصوصی و مدل کسب‌وکار *HotCodes* می‌تواند به درک بهتر ریسک‌ها و فرصت‌های موجود در استفاده از این نرم‌افزارها کمک کند.

بررسی امنیت و حریم خصوصی HotVPN،NumberBox

۱- *NumberBox* توسعه‌دهنده *HotCodes*:

جمع‌آوری داده‌ها:

اطلاعات فنی دستگاه: هنگام درخواست به‌روزرسانی آنلاین، مدل دستگاه و نسخه کلاینت جمع‌آوری می‌شود تا اطمینان حاصل شود که نسخه‌های به‌روز و سازگار برای دستگاه کاربر ارائه می‌شود.

اطلاعات تماس: در برخی نسخه‌های اپلیکیشن، ممکن است به اطلاعات مخاطبین کاربر دسترسی داشته باشد.

شناسه‌های دستگاه: شامل شماره شناسایی دستگاه اندروید، آدرس *IP* ، نام دستگاه و نسخه سیستم‌عامل.

اطلاعات مربوط به خطاها: در صورت بروز خطا، اطلاعاتی مانند آدرس *IP* دستگاه، نام دستگاه، نسخه سیستم‌عامل، پیکربندی اپلیکیشن و زمان و تاریخ استفاده از سرویس جمع‌آوری می‌شود.

سیاست‌های امنیتی:

- **استفاده از ابزارهای شخص ثالث**: اپلیکیشن از سرویس‌های شخص ثالثی مانند *Google Play Services*، *AdMob*، *Google Analytics for Firebase* و *Firebase Crashlytics* استفاده می‌کند که ممکن است اطلاعاتی را برای شناسایی کاربر جمع‌آوری کنند.

- **حفظ امنیت اطلاعات**: توسعه‌دهنده اعلام کرده است که از روش‌های قابل قبول تجاری برای حفاظت از داده‌ها استفاده می‌کند، اما هیچ روشی برای انتقال یا ذخیره‌سازی الکترونیکی اطلاعات ۱۰۰٪ امن و قابل اعتماد نیست.
- **عدم جمع‌آوری اطلاعات شخصی** :اپلیکیشن اعلام کرده است که هیچ اطلاعات شخصی یا قابل شناسایی از کاربران جمع‌آوری نمی‌کند و تنها اطلاعات فنی مورد نیاز برای عملکرد بهینه جمع‌آوری می‌شود.

حریم خصوصی کاربران:

- **حذف اطلاعات ارسال‌شده توسط کاربر**: کاربران می‌توانند درخواست حذف هرگونه اطلاعات ارسال‌شده توسط خود را کنند و در صورت تأیید، شماره از پایگاه داده حذف می‌شود.
- **عدم دسترسی به مخاطبین**: اپلیکیشن به‌طور مستقیم به مخاطبین کاربر دسترسی ندارد، اما ممکن است از اطلاعات مخاطبین برای شناسایی تماس‌های ناشناس استفاده کند.

۲- ***HotVPN*** **توسعه‌دهنده** ***HotCodes*** **:**

جمع‌آوری داده‌ها:

- **اطلاعات شخصی شناسایی‌شده**: ممکن است از کاربران خواسته شود تا اطلاعاتی مانند نام، آدرس ایمیل و تاریخچه خرید محصولات و خدمات را ارائه دهند.
- **اطلاعات مربوط به خطاها**: مشابه ***NumberBox***، در صورت بروز خطا، اطلاعاتی مانند آدرس ***IP*** دستگاه، نام دستگاه، نسخه سیستم‌عامل، پیکربندی اپلیکیشن و زمان و تاریخ استفاده از سرویس جمع‌آوری می‌شود.

سیاست‌های امنیتی:

- **استفاده از ابزارهای شخص ثالث**: اپلیکیشن از سرویس‌های شخص ثالثی مانند ***Google Play Services***، ***AdMob***، ***Google Analytics for Firebase***، ***Firebase Crashlytics*** استفاده می‌کند که ممکن است اطلاعاتی را برای شناسایی کاربر جمع‌آوری کنند.
- **عدم ارائه ویژگی‌های امنیتی استاندارد**: برخی از ویژگی‌های امنیتی استاندارد مانند ***Kill Switch*** یا ***Split Tunneling*** در این اپلیکیشن وجود ندارد که ممکن است نگرانی‌هایی را در مورد امنیت اتصال ایجاد کند.
- **عدم شفافیت در سیاست‌های لاگ‌برداری**: اگرچه اپلیکیشن ادعا می‌کند که هیچ‌گونه لاگ ترافیکی را ذخیره نمی‌کند، اما در سیاست‌های حریم خصوصی، اطلاعاتی مانند نام، ایمیل و تاریخچه خرید ذخیره می‌شود که ممکن است نگرانی‌هایی را در مورد حریم خصوصی کاربران ایجاد کند.

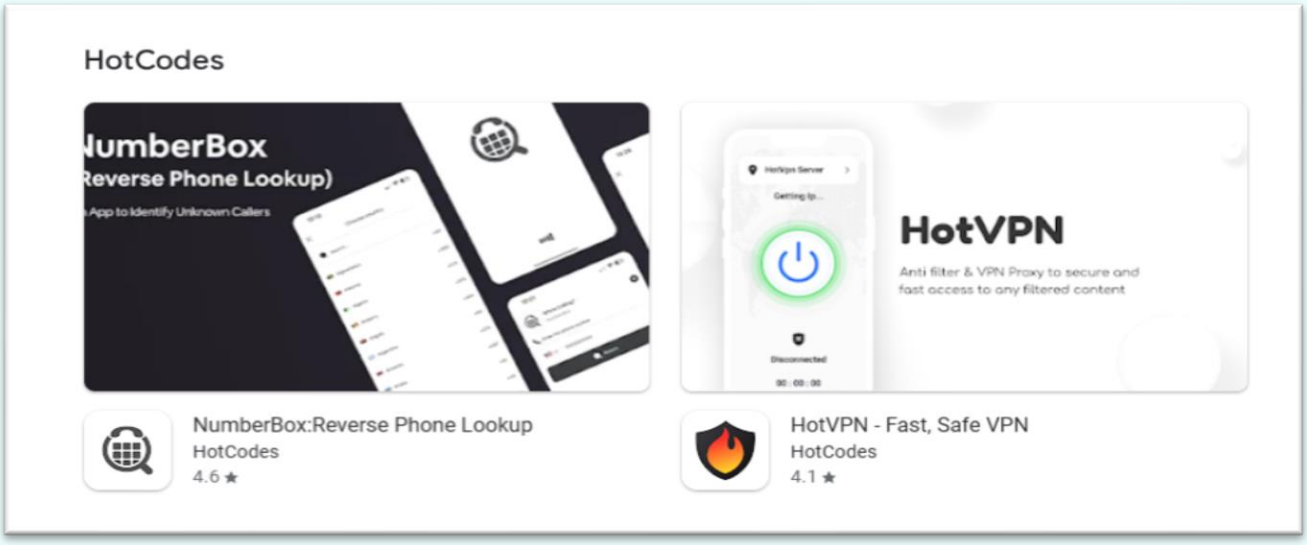
حریم خصوصی کاربران:

عدم شفافیت در محل ذخیره‌سازی داده‌ها :اطلاعات دقیقی در مورد محل ذخیره‌سازی داده‌های کاربران ارائه نشده است که ممکن است نگرانی‌هایی را در مورد حفاظت از داده‌ها ایجاد کند.

جمع‌بندی:

هر دو اپلیکیشن *NumberBox* و *HotVPN* توسط توسعه‌دهنده مشترک *HotCodes* ساخته شده‌اند و از ابزارهای شخص ثالث مشابهی برای جمع‌آوری و پردازش داده‌ها استفاده می‌کنند. در حالی که *NumberBox* ادعا می‌کند هیچ اطلاعات شخصی از کاربران جمع‌آوری نمی‌کند، اما در عمل ممکن است اطلاعاتی مانند شناسه دستگاه و اطلاعات تماس جمع‌آوری شود. از سوی دیگر، *HotVPN* با وجود ادعای عدم ذخیره‌سازی لاگ، اطلاعاتی مانند نام و ایمیل کاربران را ذخیره می‌کند که ممکن است نگرانی‌هایی را در مورد حریم خصوصی ایجاد کند.

با توجه به این نکات، کاربران باید پیش از استفاده از این اپلیکیشن‌ها، سیاست‌های حریم خصوصی و امنیتی آن‌ها را به‌دقت مطالعه کرده و با آگاهی کامل از آن‌ها استفاده کنند.



دوگانگی نیاز و تهدید در فرهنگ ارتباطات تلفنی ایران

با توجه به یکپارچگی فزاینده‌ی بانک‌های اطلاعاتی و قابلیت شماره‌گیری و شناسایی مستقیم افراد از طریق اپلیکیشن‌های تلفن همراه، موضوع حریم خصوصی در کشورهایی همچون ایران با چالش‌های مضاعفی روبه‌رو است. در فرهنگ ارتباطی ایران، کاربران غالباً هنگام ذخیره‌سازی شماره تماس‌ها، توضیحاتی در خصوص نسبت خانوادگی، موقعیت شغلی یا نوع ارتباط اجتماعی درج می‌کنند (برای نمونه: «علی – همکار اداره»، «مینا – همسایه» یا «مهندس رضایی – کارفرما»). این الگوی بومیِ ذخیره‌سازی سبب می‌شود تا در صورت دسترسی نرم‌افزارها به فهرست مخاطبین، داده‌هایی فراتر از شماره تلفن گردآوری گردد؛ داده‌هایی که می‌تواند شبکه‌های ارتباطی، جایگاه شغلی و حتی روابط شخصی افراد را آشکار سازد. در نتیجه، ساختار داده‌ای حاصل از این

فرهنگ کاربری، زمینه‌ساز نقض گسترده‌ی محرمانگی اطلاعات و بروز تهدیداتی نظیر مهندسی اجتماعی، سوءاستفاده تجاری، جعل هویت و جاسوسی سازمان‌یافته می‌شود .

ریسک‌های امنیتی در بستر شماره‌گیری و تماس درون‌برنامه‌ای

اپلیکیشن‌های شناسایی و مدیریت تماس

علاوه بر دسترسی به فهرست مخاطبین، در برخی نسخه‌ها امکان برقراری تماس مستقیم یا درون‌برنامه‌ای (VoIP)را نیز فراهم می‌کنند. در سیستم‌عامل اندروید، این امر از طریق مجوزهایی نظیر CALL_PHONE یا READ_CONTACTS انجام می‌شود که به اپلیکیشن اجازه می‌دهد مستقیماً با شماره‌های ذخیره‌شده تماس بگیرد یا آنها را به سرور ارسال کند. در مدل تماس‌های VoIP (Voice over Internet Protocol) ، داده‌های صوتی از طریق بستر اینترنت و معمولاً از سرورهای شرکت توسعه‌دهنده عبور می‌کند. به‌کارگیری این زیرساخت به‌ویژه در اپلیکیشن‌های خارجی، می‌تواند منجر به انتقال متادیتا، محتوای تماس و الگوهای ارتباطی کاربران به سرورهایی خارج از کشور گردد. این اطلاعات شامل شماره‌های تماس گرفته‌شده، مدت مکالمه، موقعیت زمانی و حتی شناسه‌های دستگاه کاربر است .

در چنین شرایطی، تهدیدات متعددی متوجه حریم خصوصی و امنیت ملی می‌شود. از جمله می‌توان به امکان شنود غیرمجاز تماس‌ها، تحلیل رفتاری(behavioral profiling) ، استخراج شبکه ارتباطی افراد و ردیابی موقعیت جغرافیایی کاربران اشاره کرد. افزون بر آن، ترکیب داده‌های تماس با اطلاعات موجود در پایگاه داده مخاطبین (که معمولاً شامل عنوان شغلی یا نسبت خانوادگی است)، می‌تواند به بازسازی دقیق روابط اجتماعی و شغلی افراد منجر شود. این مسئله نه‌تنها حریم خصوصی کاربران عادی را تهدید می‌کند، بلکه برای مدیران و مسئولان سازمانی خطر افشای اطلاعات طبقه‌بندی‌شده، جاسوسی اطلاعاتی و هدف‌گذاری مهندسی اجتماعی را نیز به همراه دارد.

در عین حال، مدیران و مسئولان ارشد سازمانی و دولتی از جمله گروه‌هایی هستند که به دلیل حجم بالای تماس‌های ناشناس، نیاز بیشتری به ابزارهای هوشمند شناسایی تماس احساس می‌کنند. این نرم‌افزارها می‌توانند در غربال‌گری تماس‌های ضروری از مزاحم یا تبلیغاتی مؤثر باشند، اما در سطح مدیریتی و امنیتی، ریسک‌های قابل‌توجهی ایجاد می‌کنند. ذخیره و پردازش فهرست تماس‌ها در سرورهای خارجی ممکن است منجر به افشای شبکه‌های ارتباطی، ردیابی رفتاری یا استخراج الگوهای تصمیم‌گیری مدیران گردد. چنین مخاطراتی، به‌ویژه در غیاب قوانین جامع حفاظت از داده در ایران، ضرورت توسعه‌ی راهکارهای بومی، ایمن و مستقل از بسترهای خارجی را برای مدیریت تماس‌ها و صیانت از داده‌های ارتباطی مدیران ارشد به‌شدت برجسته می‌سازد.

از این‌رو، ضرورت دارد استفاده از چنین اپلیکیشن‌هایی در ایران در چارچوب سیاست‌های امنیتی بومی و سامانه‌های داخلی با کنترل داده‌ها بازتعریف گردد تا خطر نشت اطلاعات ارتباطی به حداقل برسد.


WHO
Caller ID and Spam Blocker
IDENTIFIED BY WHO
Protected Over 100 Million Calls