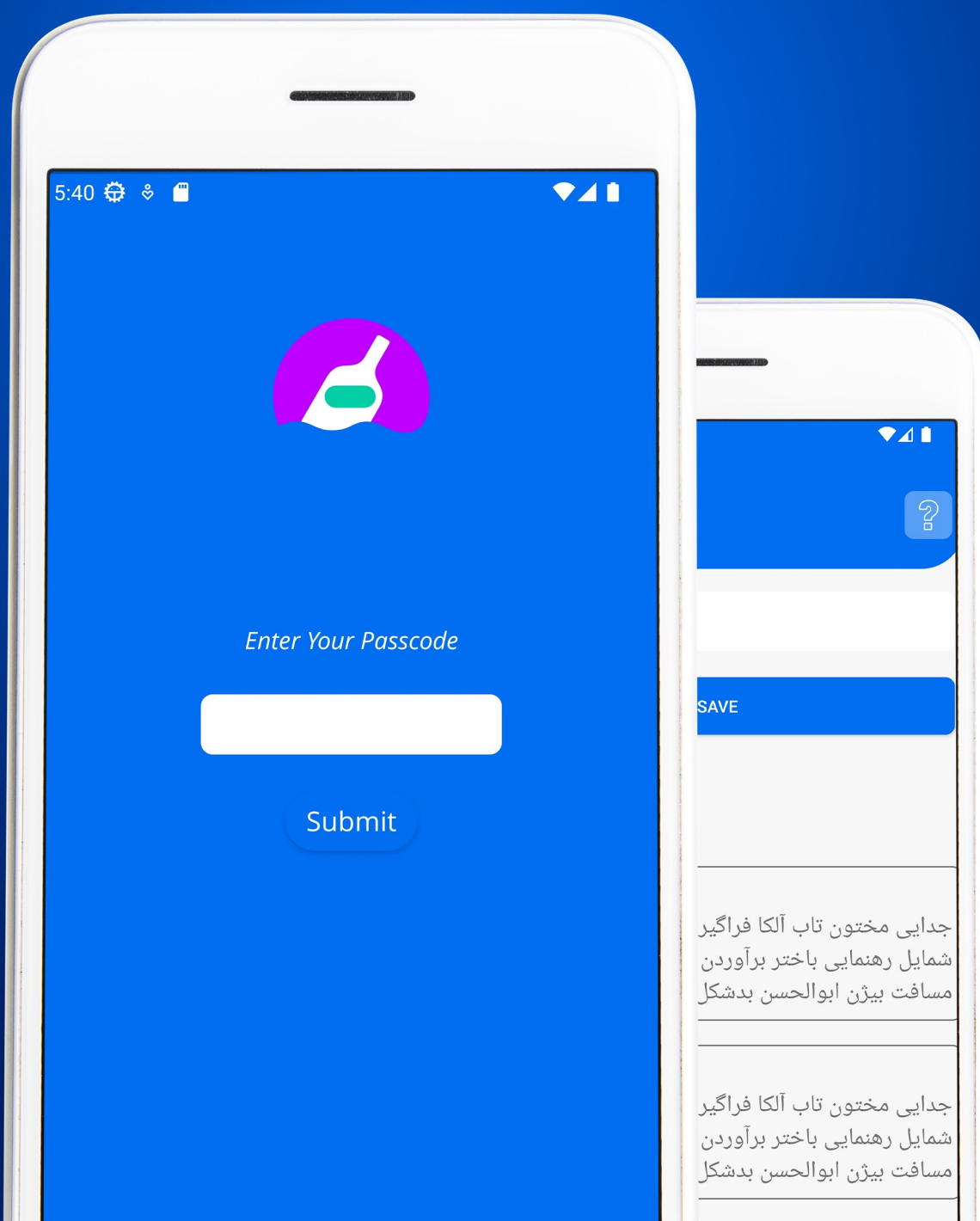
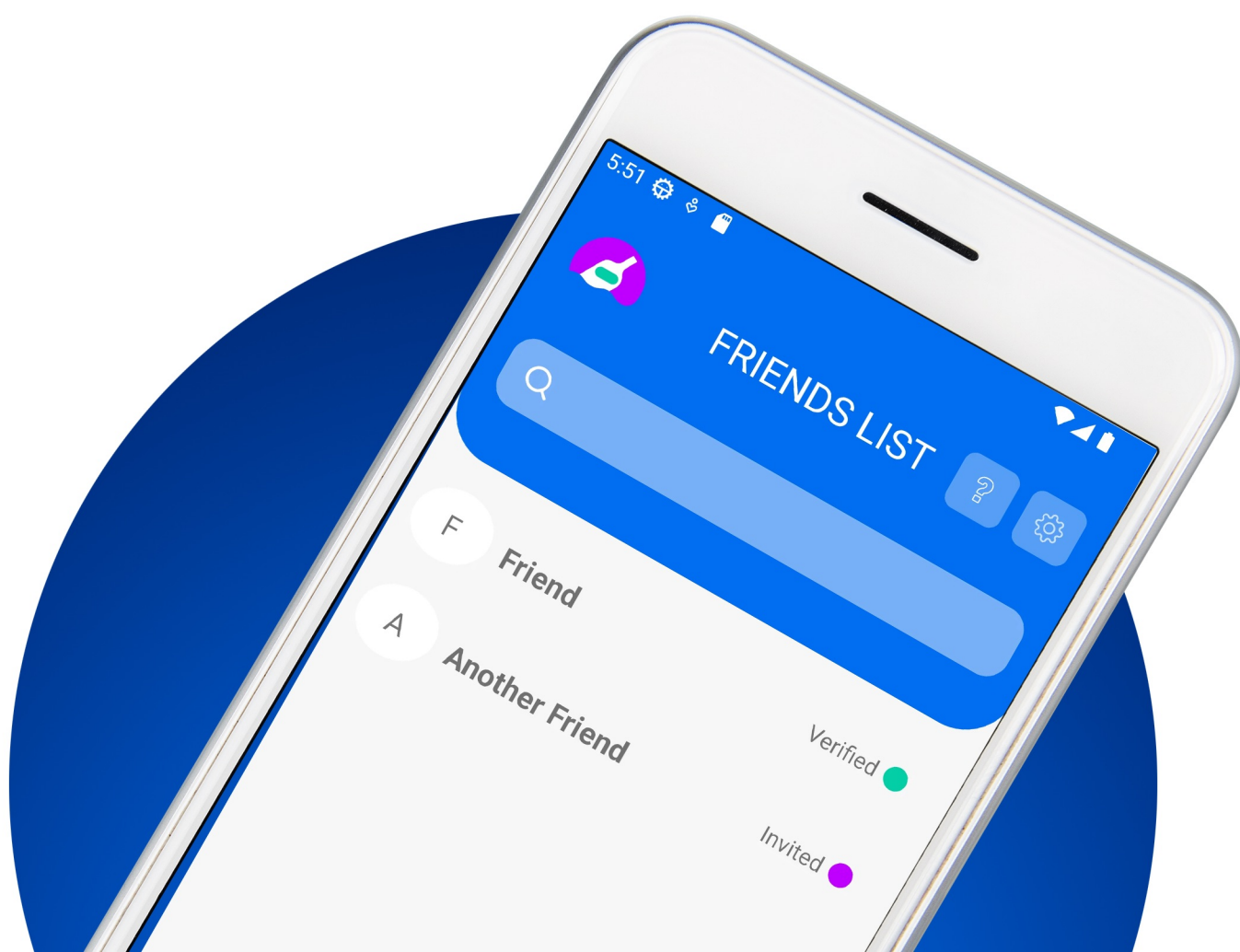


راهنمای استفاده از اپلیکیشن نهفت



اپلیکیشن نهفت ابزاری امن برای رمزنگاری و رمزگشایی پیام‌های حساس است. این برنامه بدون نیاز به اینترنت کار می‌کند و حتی در شرایط قطع کامل اینترنت نیز کاربرد دارد. در چنین شرایطی، اگر مجبور باشید پیام‌های خود را از طریق پیام‌رسان‌های داخلی یا SMS ارسال کنید، می‌توانید با استفاده از نهفت پیام‌هایتان را رمزنگاری کرده و با خیال راحت منتقل کنید. در ادامه مراحل نصب و استفاده از اپلیکیشن توضیح داده شده است.



نصب اپلیکیشن

برای دانلود و نصب نهفت می‌توانید از روش‌های زیر استفاده کنید:

▲ اندروید: از Google Play

▲ آیفون: از App Store

▲ دانلود مستقیم: از وبسایت نهفت به آدرس

www.nahoftapp.com



افزودن مخاطب

- ▲ اپلیکیشن را باز کنید.
- ▲ روی علامت + بزنید.
- ▲ نام مخاطب را وارد کرده و ذخیره کنید.
- ▲ سپس روی نام مخاطب کلیک کنید.

Android



برای افزودن مخاطب روی
علامت مثبت کلیک کنید

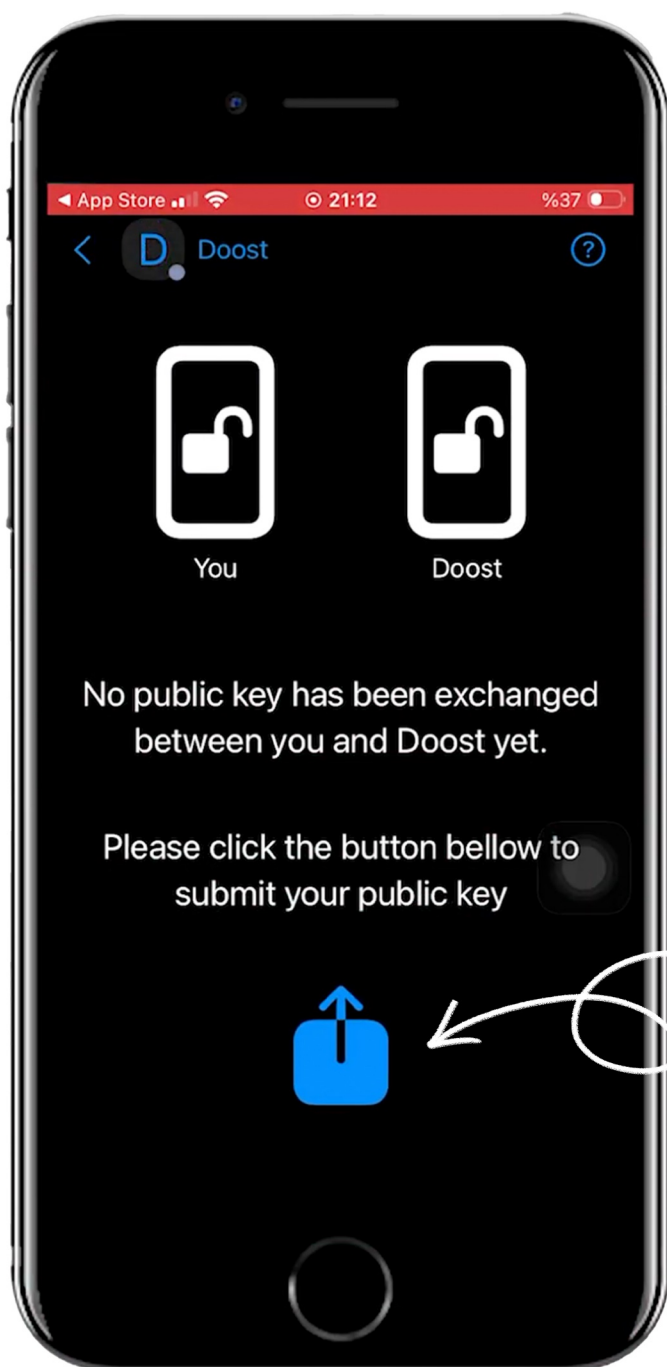
IOS



برای افزودن مخاطب روی
علامت مثبت کلیک کنید

تبادل کلید عمومی

- ▲ وارد صفحه مخاطب شوید.
- ▲ دکمه پایین صفحه را بزنید.
- ▲ کلید عمومی شما نمایش داده می شود.



iOS

پس از زدن دکمه،
می توانید کلید عمومی
را کپی کنید یا از
طریق اپلیکیشن های
پیشنهادی ارسال کنید.

Android

دکمه پایین فقط کلید
عمومی را کپی می‌کند.
سپس باید آن را از طریق
اپلیکیشن دلخواه (پیام
رسان، SMS، ایمیل و...)
پیست و ارسال کنید.



▲ بعد از تأیید، اتصال امن بین شما و مخاطب برقرار
می‌شود.

رمزنگاری و ارسال پیام

- ▲ پس از برقراری اتصال، متن پیام را بنویسید.
روی دکمه ارسال بزنید.
- ▲ پیام شما به صورت یک رشته کلمات رمزنگاری شده تولید می‌شود.
- ▲ این پیام را می‌توانید از طریق پیام‌رسان‌ها، SMS یا ایمیل ارسال کنید.



دریافت و رمزگشایی پیام

- ▲ پیام رمزنگاری شده را کپی کنید.
- ▲ وارد اپلیکیشن شوید.
- ▲ روی دکمه بالا سمت راست بزنید و پیام را پیست کنید.
- ▲ متن رمزگشایی شده و به صورت خوانا نمایش داده می شود.

Android



iOS



مدیریت مخاطبان و امنیت بیشتر

برای حذف یک مخاطب و پاک کردن سابقه پیام‌های رمزنگاری شده با او، در صفحه اصلی روی نام مخاطب از راست به چپ بکشید.



در بخش تنظیمات می‌توانید:

- ▲ رمز عبور برای ورود به اپلیکیشن تعیین کنید.
- ▲ یک رمز نابودی مشخص کنید. با وارد کردن این رمز به جای رمز عبور، تمام داده‌های نهفت به طور کامل حذف می‌شوند.



پرسش و پاسخ‌های امنیتی

اگر پیامی را از طریق یک پیام‌رسان مثل تلگرام ارسال کنم، آیا مدیران تلگرام می‌توانند پیام من را بخوانند؟

خیر. پیام‌ها در نهفت رمزنگاری می‌شوند. آن‌ها یا به صورت رشته‌ای از کلمات بی‌معنا (که هیچ ارتباطی با متن اصلی شما ندارند) یا در قالب یک عکس انتخابی شما نمایش داده می‌شوند. مدیر تلگرام می‌تواند آن متن یا عکس را ببیند، اما بدون کلید خصوصی شما (که به طور امن روی گوشی ذخیره شده) قادر به خواندن پیام نخواهد بود.



**اگر اپلیکیشن را حذف کنم و بعد گوشی من
به دست شخص دیگری بیفتد، آیا او می‌تواند
پیام‌هایی را که قبلاً فرستاده‌ام بخواند؟**

خیر. برای رمزگشایی پیام‌های شما، مهاجم به
کلید خصوصی شما نیاز دارد که روی گوشی ذخیره
می‌شود. با حذف اپلیکیشن، کلید خصوصی هم
پاک می‌شود. در نتیجه هیچ راهی برای رمزگشایی
پیام‌هایی که با آن کلید فرستاده‌اید وجود نخواهد
داشت.



آیا نصب این اپلیکیشن امن است؟

پاسخ این پرسش بستگی به شرایط و مدل تهدید شخصی شما دارد. ما بر این باوریم که نصب نهفت امن است و هرگز اپلیکیشنی منتشر نمی‌کنیم که به نظرمان ناامن باشد. اقدامات متعددی برای اطمینان از امنیت انجام شده است:

اپلیکیشن با همکاری مستقیم کاربران داخل کشور
طراحی و آزمایش شده تا با استانداردهای امنیتی آنها مطابقت داشته باشد.

یک ممیزی امنیتی (امنیت کد، رمزنگاری و روش‌های پوشان‌سازی پیام‌ها) روی اپلیکیشن انجام شده است.

نکته مهم: تنها نسخه‌ای که از Google Play Store

دانلود شود قابل اعتماد است. دریافت اپلیکیشن از منابع ناشناس یا به صورت فایل نصب (sideload) ممکن است خطرناک باشد، زیرا احتمال دارد نسخه جعلی و آلوده به بدافزار باشد.

اگر نگران هستید که داشتن اپلیکیشن روی گوشی در صورت توقیف موبایل برایتان دردسر ایجاد کند، این موضوع بستگی به شرایط شما دارد. تاکنون هیچ گزارشی مبنی بر مشکل ساز بودن نصب نهفت یا وجود قوانین رسمی علیه داشتن این اپلیکیشن دریافت نشده است. در صورت نگرانی، می‌توانید اپلیکیشن را نصب کنید، آن را امتحان کنید و بعد در صورت لزوم حذف کنید.



نهفت چه تفاوتی با سیگنال دارد؟

سیگنال یک پیام‌رسان است اما نهفت پیام‌رسان نیست؛ بلکه ابزاری است برای افزودن امنیت به پیام‌ها، حتی اگر آن‌ها را از طریق پیام‌رسان‌های ناامن داخلی بفرستید.

همچنین سیگنال در زمان قطع اینترنت کارایی ندارد، زیرا همه پیام‌های آن از طریق سرورهای بین‌المللی ارسال می‌شوند و در شرایطی که ارتباط جهانی قطع باشد، این سرورها در دسترس نیستند.

بنابراین، سیگنال و نهفت دو ابزار متفاوت برای شرایط متفاوت‌اند. حتی در صورت در دسترس بودن سیگنال، کاربران می‌توانند پیام‌های رمزنگاری‌شده نهفت را از طریق آن ارسال کنند.

وضعیت ممیزی امنیتی

▲ نسخه نخست نهفت توسط شرکت Cure53 ممیزی امنیتی شد. همه مشکلات امنیتی شناسایی شده قبل از انتشار عمومی برطرف شدند.

▲ پس از انتشار اولیه، تغییرات جدیدی مانند طراحی تجربه کاربری و افزودن قابلیت تاریخچه پیام‌ها انجام شد. این نسخه هنوز ممیزی امنیتی نشده است.

▲ در حال حاضر، تیم توسعه دهنده در حال آماده سازی نسخه جدید نهفت است و برای انجام ممیزی امنیتی با شرکت Radically Open Security وارد مذاکره شده‌اند. در این ممیزی، علاوه بر بررسی کدهای جدید، پرسش‌های امنیتی مهمی مثل میزان امنیت تاریخچه پیام‌ها نیز بررسی خواهد شد.



این راهنما توسط تیم تولید محتوای
مجموعه فعالیت امن تهیه شده است.

پاییز ۱۴۰۴