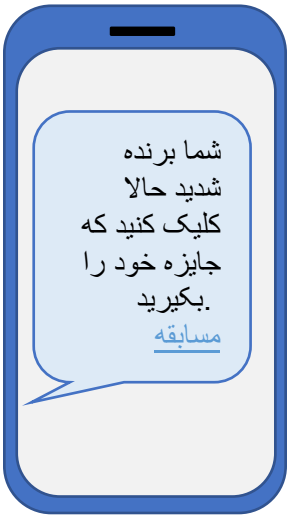
Grassroots Digital Hub

نکات ایمنی تلفن



مراقب موارد زیر باشید...

- تماس‌ها و پیامک‌ها (SMS) از شماره‌هایی که نمی‌شناسید.
- پیامی که باعث می‌شود خیلی خوشحال یا خیلی بترسید.
- تماس‌گیرنده یا پیامکی که شما را تحت فشار می‌گذارد تا سریع کاری انجام دهید
- پیامکی که از شما می‌خواهد روی یک لینک کلیک کنید
- اگر قبل از شروع صحبتِ تماس‌گیرنده تأخیری وجود دارد
- اگر تماس‌گیرنده توهین‌آمیز یا تهدیدکننده است
- هرگونه درخواست پول یا اطلاعات شخصی/محرمانه

این کارها را انجام ندهید!

- هیچ‌گونه اطلاعات محرمانه‌ای ندهید، مثل شماره بیمه اجتماعی (SIN)، اطلاعات بانکی، نام کاربری یا رمز عبور.
- پول ارسال نکنید.
- روی لینک‌های ارسال‌شده کلیک نکنید.
- به پیامک پاسخ ندهید.
- با شماره‌ای که به شما داده شده تماس نگیرید و از گزینه «تماس مجدد» گوشی استفاده نکنید.

چه کار کنید

- اشکالی ندارد تماس را قطع کنید یا اجازه دهید تماس ناشناس به روی پیام گیر برود.
- شماره را مسدود (بلاک) کنید.
- اگر نگران عزیزانتان هستید، شماره واقعی آنها را پیدا کرده و خودتان تماس بگیرید.

به خاطر داشته باشید

- کلاهبرداران بسیار زیرک هستند و برای فریب شما از هر روشی استفاده می‌کنند، حتی جا زدن خود به‌جای عزیزانتان.
- دولت و بانک‌ها وقتی با شما تماس می‌گیرند، از شما اطلاعات شخصی درخواست نمی‌کنند. اگر شما با آن‌ها تماس بگیرید، ممکن است برای تأیید هویت این اطلاعات را بپرسند.
- شرکتی که به شما فشار می‌آورد، شایسته کسب‌وکار شما نیست.

چه چیزهایی ممکن است ببینید یا بشنوید

- **درخواست کمک:** طوری به نظر می‌رسد که تماس‌گیرنده یا فرستنده پیام کسی است که می‌شناسید و واقعاً به کمک شما نیاز دارد؛ معمولاً می گویند پول لازم دارند و اگر کمک نکنید، اتفاق بدی برای او می‌افتد.
  - تماس‌گیرنده یا پیامک با این روش‌ها اعتماد شما را جلب می‌کند:
    - هم رسانی اطلاعات شخصی شما یا خانواده‌تان (که از شبکه‌های اجتماعی پیدا کرده‌اند)
    - صحبت کردن دقیقاً شبیه عزیزان یا دوستان شما (ممکن است هوش مصنوعی باشد)

- **تهدید:** تماس‌گیرنده یا پیامک تهاجمی و مطالبه‌گر است. ممکن است به شما گفته شود:
  - از طرف دولت یا یک نهاد حقوقی تماس گرفته‌اند
  - اگر فوراً اقدام نکنید، اتفاق بسیار بدی رخ خواهد داد
  - باید از یک وب‌سایت بازدید کنید یا اطلاعات محرمانه مثل SIN یا اطلاعات بانکی را ارائه دهید

- **خبرهای عالی!** تماس‌گیرنده یا پیامک ممکن است بگوید پیشنهاد ویژه‌ای فقط برای شما دارد، یا برنده مسابقه شده‌اید، یا پولی در راه است. اگر سؤال بپرسید یا تأخیر کنید، ممکن است تهاجمی شوند یا توهین کنند. ممکن است از شما بخواهند:
  - سریع اقدام کنید
  - روی یک لینک کلیک کنید یا اطلاعات شخصی ارائه دهید

- **پیشنهاد کمک:** تماس‌گیرنده یا پیامک ممکن است بگوید از طرف بانک شما یا خدمات کامپیوتری است. ممکن است به شما گفته شود:
  - دستگاه یا حساب شما هک شده است («به خطر افتاده»)
  - برای دریافت کمک باید روی یک لینک کلیک کنید یا اطلاعات محرمانه بدهید
  - اگر تأخیر کنید، پول یا خدمات خود را از دست خواهید داد

اگر این اتفاق برای شما افتاد

- اگر نام کاربری و گذرواژه خود را به اشتراک گذاشته‌اید، سعی کنید فوراً آن‌ها را تغییر دهید.
- اگر اطلاعات بانکی یا کارت اعتباری خود را به اشتراک گذاشته‌اید، فوراً بانک خود را مطلع کنید.
- به پلیس و سیستم گزارش‌دهی آنلاین مرکز مقابله با کلاهبرداری کانادا (Canadian Anti-Fraud Centre's online reporting system) گزارش دهید یا با شماره 1-888-495-8501 تماس بگیرید.
- دوستان و اعضای خانواده را از آنچه برای شما رخ داده مطلع کنید تا احتمال وقوع آن برای آن‌ها کمتر شود.

.

SSHRC CRSH
Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada

NSERC CRSNG

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council.