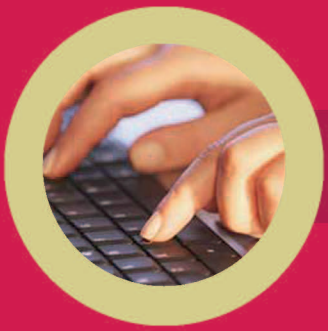
CYBER POLICE

پلیس فضای تولید و تبادل اطلاعات ناجا

راهنمای ۱۰ گامی پلیس فتا برای تامین امنیت آنلاین خانواده

چگونه با خردسالان، کودکان و نوجوانان و هر شخص تازه‌کار در مورد امنیت آنلاین سخن بگویید.



معرّفی

میلیون‌ها خانواده در سرتاسر دنیا هر روز از اینترنت برای یادگیری، پژوهش، خرید و فروش، استفاده از خدمات بانکی، سرمایه‌گذاری، به اشتراک گذاری عکس، بازی کردن، دانلود فیلم و موزیک، ارتباط با دوستان، آشنا شدن با افراد جدید و مشارکت در میزبانی برای سایر فعّالیّت‌ها استفاده می‌کنند. گرچه فضای مجازی مزایا، فرصت‌ها و آسودگی‌های متعدّدی را به ارمغان می‌آورد، امّا با رشد رو به افزایشی خطرناک است به طوری که روزانه بسیاری از تهدیدهای جدید ظهور و بروز می‌یابند.

جای تعجّب نیست که مجرمان اینترنتی به دنبال استفاده از اینترنت و کسانی هستند که آن را به کار می‌برند. شما و اعضای خانواده‌ی شما نیاز دارید که هر زمان که آنلاین می‌شوید در امنیت باشید.

علاوه بر نصب نرم‌افزارهای امنیتی قوی از محصولات شرکت‌های قابل اعتماد برای دفاع از خانواده‌ی خود در برابر هکرها، سارقان هویّت، کلاهبرداران ایمیلی و تبه کاران، شما باید برخی از قوانین ابتدایی ایمنی در اینترنت را نیز دنبال کرده و از قدرت تعقّل خود استفاده کنید. شما به یک برنامه‌ی امنیت اینترنتی برای خانواده ی خود نیاز دارید.

به محض آن که یکی از اعضای خانواده، فعّالیّت‌های آنلاین خود را آغاز می‌کند، فارغ از آن که چه سنّ و سالی دارد، زمان آموزش وی درباره‌ی امنیت سایبری فرا می‌رسد. شما باید آگاه باشید که اگر حتّی در خانه کامپیوتر ندارید، کامپیوترهای شخصی تقریباً در هر جایی هستند. در مدارس، کتابخانه‌ها، خانه‌ی دوستان، خانه‌ی خویشاوندان و تقریباً در همه جا. این که هر کسی دانش ابتدایی حفاظت از خود در فضای سایبری را بداند، بسیار مهم است.

اینترنت امروزی:
ادامه با احتیاط

- شانس شما برای این که یکی از قربانیان جرایم سایبری باشید، یک به چهار است.

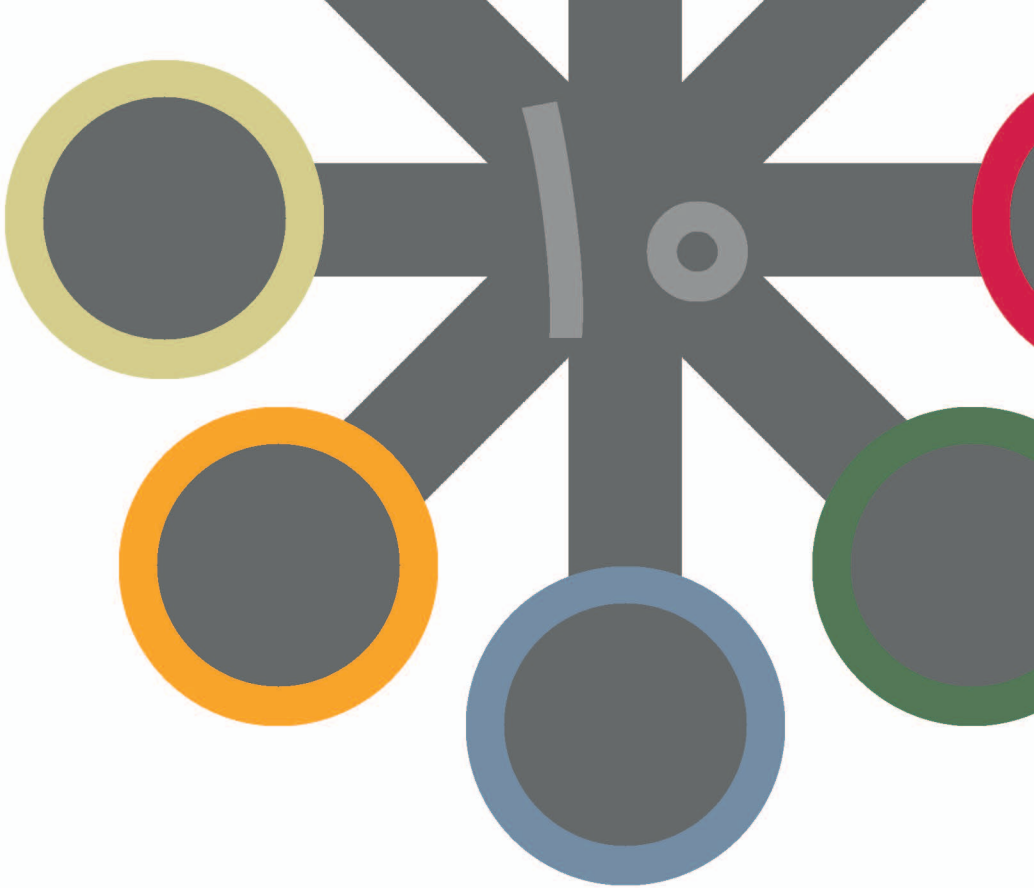
- هکرها، هر ۳۹ ثانیه یک بار، کامپیوترهای متصّل به اینترنت را مورد حمله قرار می‌دهند.

- بر اساس گزارش لابراتوارهای امنیتی، ۲۲۲۰۰۰ ویروس رایانه‌ای شناخته شده وجود دارند و شمار تهدیدها نیز روزانه افزایش می یابد.

- ویروس‌های رایانه‌ای در دو سال گذشته ۱.۸ میلیون خانوار را مجبور کرده‌اند تا رایانه‌هایشان را تعویض کنند.

- در سال ۲۰۰۶، ۸.۹ میلیون آمریکایی قربانیان جرایم مرتبط با هویت (جعل هویّت، سرقت هویّت و ...)

- ٪۷۱ از افراد ۱۳ تا ۱۷ ساله پیام‌های آنلاینی از افرادی دریافت کرده‌اند که آنان را نمی‌شناسند.

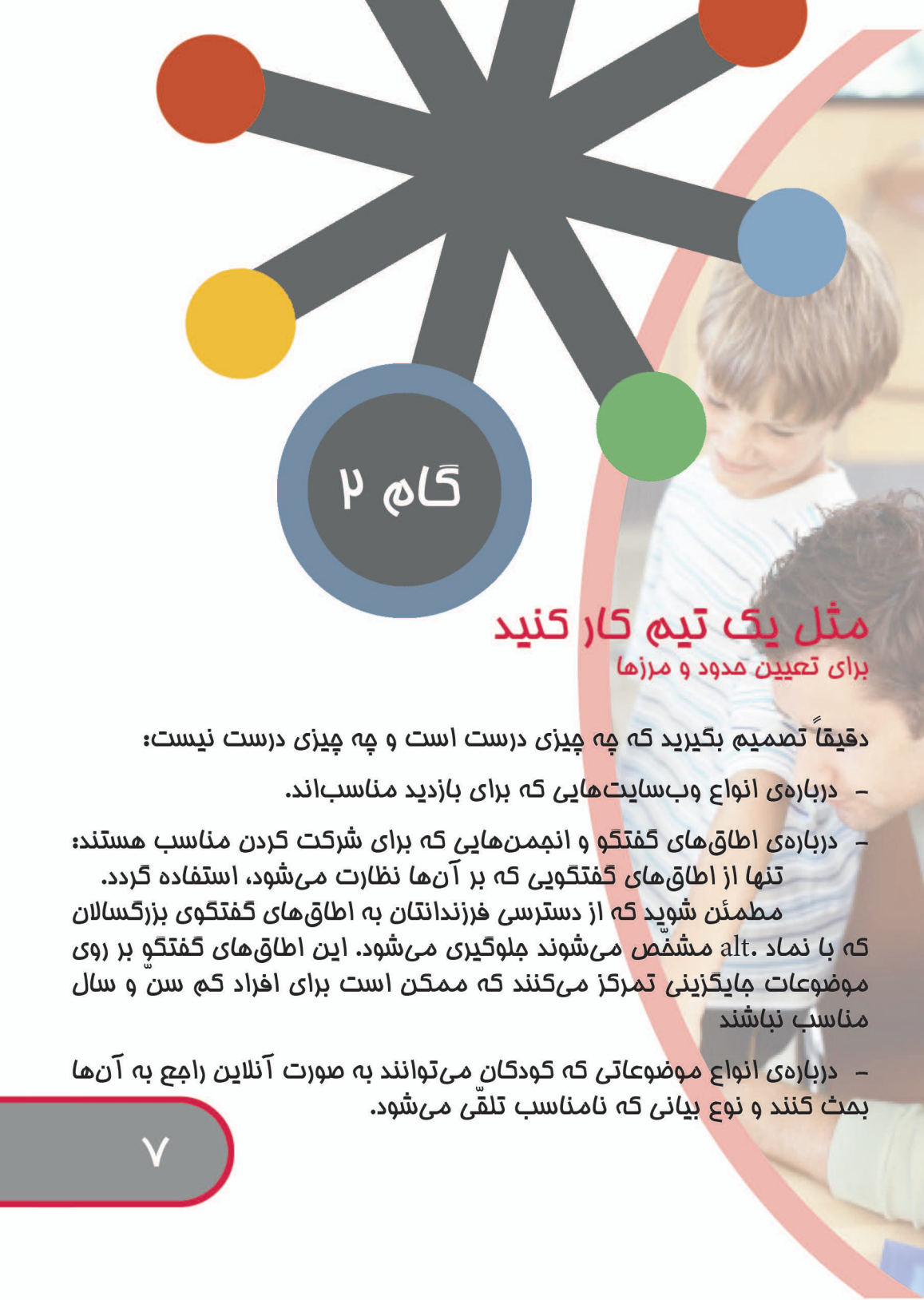


یک برنامه‌ی ده‌گامی برای کمک به حفاظت از اعضای خانواده شما

گام ۱

گام یک: جانمایی رایانه

در خانه‌ای که کودکان در آن حضور دارند، جایی که رایانه‌ی خانواده را در آن قرار می‌دهید، یکی از مهم‌ترین تصمیماتی است که بایستی اتّخاذ کنید. ما توصیه می‌کنیم که رایانه را در یک فضای پر تردّد از محیط خانه قرار دهید و تعداد ساعت‌هایی را که کودکان صرف آن می‌کنند، محدود کنید. مطمئن شوید که نرم‌افزارهای امنیتی رایانه‌ای که شامل ابزارهای نظارت و کنترل والدین هم هستند؛ نظیر آنتی‌ویروس‌ها و نرم‌افزارهای امنیت اینترنت (Internet Security) را در اختیار دارید.



گام ۲

مثل یک تیم کار کنید

برای تعیین حدود و مرزها

دقیقاً تصمیم بگیرید که چه چیزی درست است و چه چیزی درست نیست:

- درباره‌ی انواع وب‌سایت‌هایی که برای بازدید مناسب‌اند.
- درباره‌ی اطاق‌های گفتگو و انجمن‌هایی که برای شرکت کردن مناسب هستند: تنها از اطاق‌های گفتگویی که بر آن‌ها نظارت می‌شود، استفاده گردد. مطمئن شوید که از دسترسی فرزندانتان به اطاق‌های گفتگوی بزرگسالان که با نماد .alt مشخّص می‌شوند جلوگیری می‌شود. این اطاق‌های گفتگو بر روی موضوعات جایگزینی تمرکز می‌کنند که ممکن است برای افراد کم سنّ و سال مناسب نباشند
- درباره‌ی انواع موضوعاتی که کودکان می‌توانند به صورت آنلاین راجع به آن‌ها بحث کنند و نوع بیانی که نامناسب تلقّی می‌شود.

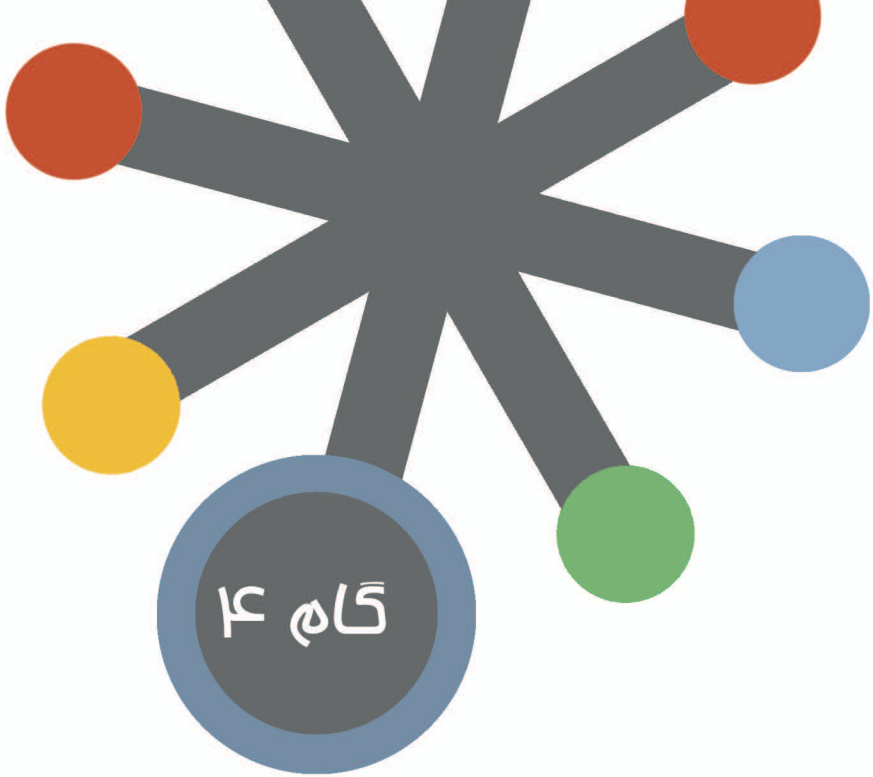
با هم ،بر اساس توافق

قوانین رایانه‌ی خانوادگی

ما موارد ذیل را توصیه می‌کنیم

- هرگز با نام کاربری¬ای که هویّت واقعی را نشان می‌دهند یا تحریک آمیزند به رایانه وارد نشوید.
- هرگز کلمه‌ی عبور خود را به نمایش نگذارید.
- هرگز شماره‌های تلفن یا آدرس‌های خود را به نمایش نگذارید.
- هرگز اطّلاعاتی را که نشان‌دهنده‌ی هویّت شماست، ارسال نکنید.
- هرگز تصاویر نامناسب یا چیزهایی که هویت شما را به نمایش می‌گذارند ارسال نکنید. (برای مثال: عکس‌هایی که در آن بر روی لباس شما نام مدرسه یا شهر شما نوشته شده‌است)
- هرگز هیچ‌گونه اطّلاعاتی را با غریبه‌هایی که آن‌ها را به صورت آنلاین می‌بینید، به اشتراک نگذارید.
- هرگز به صورت چهره به چهره با غریبه‌هایی که آن‌ها را به صورت آنلاین می‌بینید، ملاقات نکنید.
- هرگز فایل‌های رایانه‌ای متصّل شده به ایمیل‌هایی که از غریبه‌ها دریافت می کنید را باز نکنید.

زمانی که شما این قوانین را وضع کردید، یک پوستر از آن‌ها درست کنید و آن را در کنار رایانه قرار دهید.



یک قرارداد امضا کنید

برای رفتار مناسب آنلاین

یک قرارداد بنویسید یا از نمونه‌ی صفحه‌ی بعد، یا نمونه‌ی دیگری که در اختیارتان قرار خواهد گرفت، استفاده کنید؛ که در آن درک روشنی در میان اعضای خانواده در استفاده مناسب از رایانه و رفتارهای آنلاین وجود دارد.

تعهّدنامه امنیت آنلاین

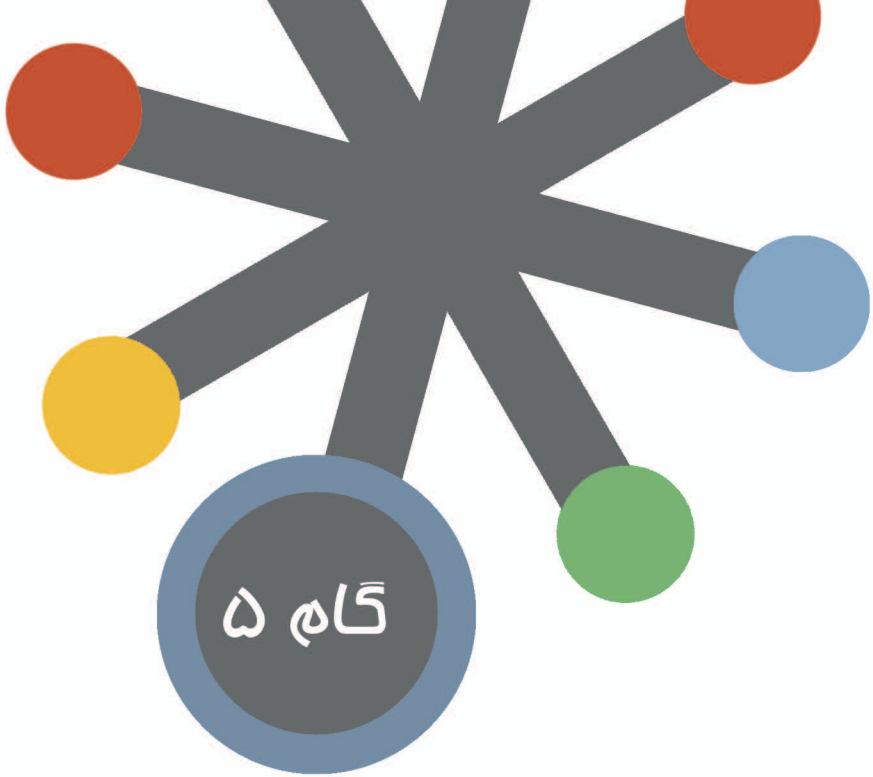
از این رو که رایانه و اینترنت امتیازی است که من نمی‌خواهم آن را از دست دهم؛

- هر زمانی که آنلاین باشم، به صورت کاملاً ایمن به گشت و گذار در اینترنت، جستجو، کار، بازی و چت خواهم پرداخت.
- من از تمامی قوانینی که بر سر آن توافق کرده‌ایم پیروی خواهم کرد.
- من نام واقعی، شماره‌ی تلفن، آدرس و کلمه‌ی عبورم را برای دوستان آنلاین به نمایش نخواهم گذاشت.
- من هرگز به صورت شخصی با افراد آنلاین ملاقات نخواهم کرد.
- اگر خود را در موقعیتی بیابم که در آن ناایمن یا ناراحت باشم، قول می‌دهم که شما را آگاه کنم. (پدر و مادرم، سرپرست یا معلّم‌ام) می‌دانم که شما می‌توانید به من کمک کنید.
- من به این تعهّدنامه وفادارم و تبعات تصمیمات خود را می‌پذیرم.

امضای کودک.....

- به عنوان پدر و مادر/ سرپرست/ معلّم، من قول می‌دهم، زمانی که تو نیاز به من به عنوان یک راه‌نما داری در دسترس تو باشم و به تو برای حلّ هر مشکلی که قادر به رفع کردن آن باشم، کمک کنم.

امضای پدر و مادر/ سرپرست/ معلّم.....



نرم‌افزارهای امنیتی را نصب کنید

مطمئن شوید که شما نرم‌افزارهای امنیتی قابل اعتماد که رایانه‌ی شما را در برابر ویروس‌ها، هکرها و جاسوس‌افزارها محافظت می‌کند، در اختیار دارید. همچنین آن بایستی محتواها، عکس‌ها و وب‌سایت‌های توهین‌آمیز را فیلتر کند. این نرم‌افزار باید به صورت مداوم به روزرسانی گردد چنان‌که تهدیدهای جدید به صورت روزانه به وجود می‌آیند. ایده‌آل است که این نرم‌افزارها، به صورت اتوماتیک به روزرسانی گردند. این بهترین انتخاب است.

از نرم‌افزارهای نظارت والدین استفاده کنید

تمامی عرضه‌کنندگان عمده‌ی نرم‌افزارهای امنیتی، نرم‌افزارهای نظارت والدین را ارائه می‌کنند. مطمئن باشید که آن‌ها را فعّال کرده‌اید. اگر شما از نرم افزارهای رایگان یا از نرم‌افزارهایی که نظارت والدین ندارند استفاده می‌کنید، نرم افزاری را برای سفارش دادن در نظر بگیرید که شامل نظارت والدین نیز می‌شود. زمانی را صرف کنید تا یاد بگیرید که این کنترل‌ها چگونه کار می‌کنند و از گزینه هایی که موارد نامناسب را فیلتر یا مسدود می‌کنند استفاده کنید. البته، این ابزارها محدودیت‌های خاصّ خود را دارند. هیچ چیز نمی‌تواند جای پدر و مادر مسؤول و پاسخگویی را بگیرد که فرزندان خود را در زمانی که آنلاین هستند مراقبت می‌کند.

به خانواده‌ی خود یادآوری کنید
که افراد آنلاین غریبه هستند.

هرکسی که آنلاین می‌شود باید بداند که:

مهم نیست که چگونه اغلب شما با دوستان آنلاین‌تان چت می‌کنید، مهم نیست که چقدر چت می‌کنید و مهم نیست که شما چقدر فکر می‌کنید که آن‌ها را می‌شناسید. مهم این است که افرادی که شما به صورت آنلاین آن‌ها را ملاقات می‌کنید غریبه هستند. خیلی ساده است که در زمانی که شما آنلاین هستید، به شما دروغ بگویند و خود را کس دیگری جا بزنند. خصوصاً کودکان لازم است بدانند که ممکن است یک «دوست» جدید، در واقعیت یک مرد چهل‌ساله باشد تا یک نفر هم سنّ و سال خودشان.

شبکه‌های اجتماعی مثل فیس‌بوک و گوگل‌پلاس یک راه حلّ ایده‌آل برای آشنایی با افراد جدید هستند. بنابراین، پدر و مادر بایستی این سایت‌ها را مشاهده کرده و پروفایل فرزندان خود را بازرسی کنند تا مطمئن شوند که صحبت های نامناسب، جایی در آن نداشته باشند و عکس‌های غیرقابل قبول ارسال نگردند. پدر و مادر بایستی مکالمات و چت‌های اینترنتی فرزندان خود را نظارت کنند تا مطمئن شوند که آنان توسّط شکارچیان آنلاین تعقیب نمی‌شوند.

گام ۸

یک کلمه‌ی عبور قوی بسازید

برای ساختن رمز عبوری که شکستن آن سخت باشد، از حدّاقل هشت کاراکتر که ترکیبی از حروف، اعداد و سمبل‌هاست، استفاده کنید. رمز عبور باید به صورت دوره‌ای تعویض شود تا احتمال به خطر افتادن یک رمز عبور در طول زمان کاهش یابد.

تکنیک‌های ساخت رمز عبورهای قوی عبارتند از:

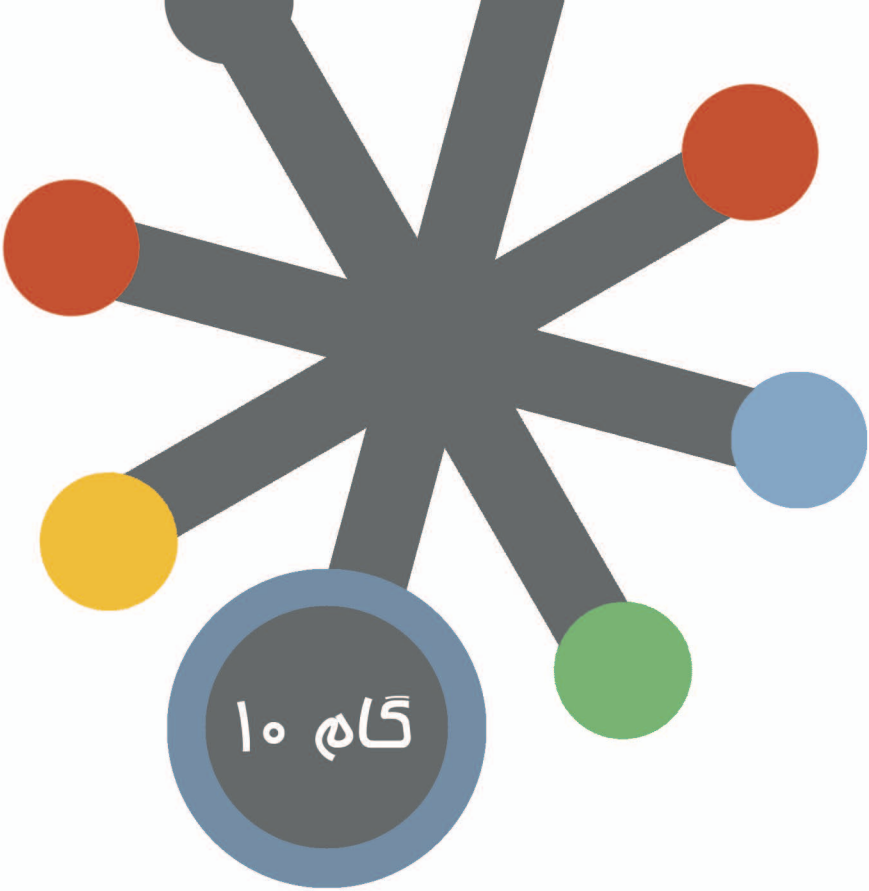
- استفاده از شماره شناسی خودرو: «GR۸wayy۲B»
- استفاده از چند کلمه‌ی کوچک به همراه علائم نگارشی: «betty,boop$car»
- قراردادن علائم نگارشی در وسط کلمه: «Roos%velt»
- استفاده از یک روش غیر معمول قراردادی در یک کلمه: «ppcrnbll»
- استفاده از حرف اوّل هر کلمه در یک عبارت به همراه یک عدد تصادفی: «hard to crack this password=htc۵tp»
- کلمه‌ی عبور خود را به اشتراک نگذارید!

گام ۹

نرم‌افزارهای امنیتی خود را کنترل کنید

هر از چندی، نرم‌افزارهای امنیتی خود را باز کنید و کنترل نمایید که رایانه‌ی شما با این سه محافظ اصلی، محافظت می‌شود: ضد ویروس، ضد جاسوس‌افزار و دیواره‌ی آتش (فایروال).

به این محافظ‌های اصلی، نرم‌افزارهایی مثل ضد اسپم و نرم‌افزارهای جستجوی امن که دارای آنتی فیشینگ و رتبه‌بندی ایمنی هم هستند بایستی افزوده شود. این ایده‌ی خوبی برای خانواده است که مجموعه‌ای از نرم‌افزارهای حفاظتی را بر روی رایانه‌شان داشته باشند که همچنین شامل نرم‌افزارهای نظارت والدین و ابزارهای جلوگیری از سرقت هویّت است.



همیشه آگاه باشید

هر چقدر بیشتر بدانید، بیشتر در امنیت خواهید بود. منابع آموزشی آنلاین از جمله سایت پلیس فتا را در آدرس www.cyberpolice.ir مطالعه کنید.

الفبای امنیت آنلاین
برای خردسالان
۳ تا ۷ ساله

کودکان

پلیس فضای تولید و تبادل اطلاعات ناجا
CYBER POLICE

الف با خردسالان صحبت کنید

وقتی که با خردسالان درباره امنیت اینترنت صحبت می‌کنید، این کار را در حالی انجام دهید که رایانه را خاموش کرده‌اید تا تمام حواس او را به خود معطوف کنید. صحبت خود را با بیان این مطلب آغاز کنید که رایانه یک ابزار و اینترنت نیز شبیه یک کتابخانه‌ی الکترونیکی فوق‌العاده بزرگ و سرشار از اطّلاعات است.

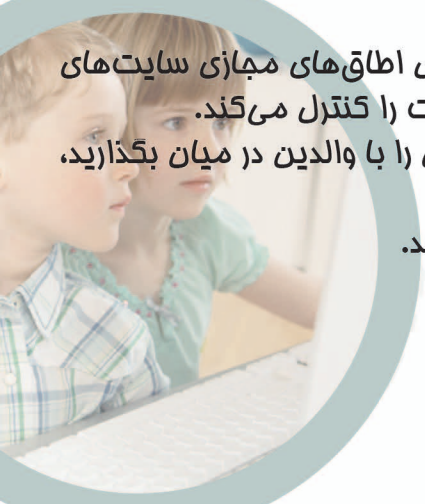
تشریح کنید که چرا امن بودن در فضای آنلاین اهمیّت دارد. به آن‌ها بگویید که رایانه می‌تواند به مثابه‌ی یک در گشوده در برابر اطّلاعات مهمِ شخصی شما باشد. به آن‌ها بگویید که چطور آدم‌بدها می‌توانند کنترل رایانه‌ی شما را در دست بگیرند و آن را نابود کنند تا جایی که شما مجبور شوید یک رایانه‌ی تازه بخرید.

برای آن‌ها بیان کنید که چرا اهمیت دارد که اطّلاعات شخصی خود را با افراد آنلاین به اشتراک نگذارند. به آن‌ها بگویید که از اسامی واقعی‌شان استفاده نکرده و درباره‌ی جایی که در آن زندگی می‌کنند یا مدرسه‌ای که می‌روند، صحبت نکنند.

ب یک لیست ویژه از قوانین کاربری رایانه برای خردسالان درست کنید

این لیست باید شامل این موارد باشد:

- موزیک یا برنامه‌ای را بدون اجازه‌ی والدین از سایت‌های اینترنتی دانلود نکنید.
- تنها از اطاق‌های گفتگوی نظارت شده مثل اطاق‌های مجازی سایت‌های کودکان استفاده کنید که یک بزرگسال فضای چت را کنترل می‌کند.
- هرگز عکسی از خود را بدون این که قبلاً آن را با والدین در میان بگذارید، ارسال نکنید.
- از کلمات و الفاظ بد و رکیک استفاده نکنید.



- سایت‌های مخصوص بزرگ‌سالان را مشاهده نکنید.
- اطّلاعات خود را تنها با کسانی به اشتراک بگذارید که آن‌ها را در دنیای واقعی می‌شناسید. مثل هم‌کلاسی‌ها، دوستان و اعضای خانواده.
- هرگز به فرم‌ها و پرسش‌نامه‌های آنلاین بدون کمک والدین پاسخ ندهید.
- تنها از موتورهای جستجوی ویژه کودکان مثل موتور جستجوی «ASK برای کودکان» و «یاهو! بچّه‌ها» استفاده کنید.

۵ از مرورگرها و موتورهای جستجویی که اختصاصاً برای کودکان طرّاحی شده‌اند استفاده کنید.

مطمئن شوید که فرزندان شما از مرورگرهایی استفاده می‌کنند که کلمات و تصاویر نامناسب را نمایش نمی‌دهند. کنترل کنید که این مرورگرها تنظیمات مرتبط با مشاهده‌ی وب‌سایت‌های ایمن و مطمئن و فیلتر کلمات نامناسب را دارا باشند. تمام آن‌چه که نیاز دارید آن است که این نرم‌افزارها را بررسی کرده و تنظیمات وب‌سایت‌های پیش‌گزیده و کلمات را تایید کنید.

الفبای امنیت آنلاین
برای خردسالان
۸ تا ۱۲ ساله

کودکان

پلیس فتای تولید و تبادل اطلاعات ناجا
CYBER POLICE

الف با کودکان خود صحبت کنید

کودکانی که در سنین هشت تا دوازده سال قرار می‌گیرند به مراتب پیچیده‌تر از زمان خردسالی خود هستند. واژه‌ی کودک به دقّت منعکس‌کننده جمعیتی از بچّه هاست که هنوز نمی‌توان واژه‌ی نوجوان را به آنان اطلاق کرد. بدانید که کودکان در استفاده از رایانه، چه در مدرسه و چه در خانه به مراتب راحت‌تر هستند.

پیش از این که شما با کودکان صحبت کنید، نیازمند این هستید که تصمیماتی را راجع به ایجاد مرزهای استفاده از اینترنت اتّخاذ کنید. برای این‌که این قوانین را وضع کنید، لازم است که آن‌ها را ابتدا تعریف کنید. برای کمک به ایمن نگه‌داشتن کودکانتان، شما بایستی به سؤال‌های زیر پاسخ دهید:

- آیا رایانه در یک فضای عمومی از خانه قرار دارد؟
- چه وب‌سایت‌هایی برای بازدید کودکان شما مناسب هستند؟
- زمانی که برای آن صرف می‌کنند چقدر باید باشد؟
- زمانی که آنلاین هستند چه کاری باید انجام دهند؟
- چه کسانی اجازه دارند که با او در تعامل و ارتباط باشند؟
- اگر شما آن‌ها را کنترل نکنید، چه وقت بایستی کمک، راهنمایی و تأیید شما را طلب کنند؟

زمانی که شما به سؤال‌های بالا پاسخ دادید، شما می‌توانید صحبت با کودکان را آغاز کنید. برای این که تمرکز و حواس کودک را به خود جلب کنید، رایانه را خاموش کنید. بایستی برای آنان تشریح کنید که رایانه یک ابزار است و ضروری است که در زمان آنلاین شدن، ایمنی آن را حفظ کنید.

مطمئن شوید که این نکات را بیان خواهید کرد:

- بحث در مورد ویروس‌ها، جاسوس‌ابزارها و هکرها
- بحث در مورد این‌که شکارچیان کودکان چگونه توجّه آنان را برای صحبت کردن در باره‌ی خودشان جلب می‌کنند.
- تشریح کنید که به دلیل این که رایانه یک در باز به سمت اطّلاعات مهم شخصی شماست، ضروری است که در هنگام آنلاین شدن از امنیت لازم برخوردار باشید.
- بحث در مورد این که سرقت هویّت به چه نحو اتّفاق می‌افتد.
- بحث در مورد این واقعیت که شما یا یک خبره‌ی رایانه (در صورتی که شما خبره نباشید) می‌توانید هرگونه اتّفاقی را که بر روی کامپیوتر می‌افتد، ردگیری کنید.
- صحبت در باره‌ی این که چگونه مجرمین می‌توانند کنترل رایانه‌ی شما را به دست بگیرند به نحوی که شما مجبور شوید، یک رایانه‌ی تازه بخرید.

ب کمک‌خواستن در زمانی که اتّفاقات ناراحت‌کننده‌ای در فضای آنلاین رخ می‌دهد.

به کودکان خود تاکید کنید که اگر در طول چت کردن خود پیام نامربوط یا نامناسبی را دریافت می‌کنند، به شما اطّلاع دهند و شما نیز در مقابل آن‌ها را دعوا نمی‌کنید و دسترسی آن‌ها به اینترنت را نیز قطع نخواهید کرد. کودکان را توجیه کنید که شما می‌دانید که آن‌ها قادر به کنترل کردن آن‌چه که دیگران می‌گویند نیستند و شما آن‌ها را به این دلیل سرزنش نخواهید کرد.

همچنین، مطمئن شوید که کودکان شما در فضای اینترنت نسبت به کودکان دیگر قلدری نمی‌کنند یا مورد قلدری قرار نمی‌گیرند. زمانی که کودکان مدرسه را ترک می‌کنند، لزوماً همکلاسی‌ها و درگیری‌هایی که با آن ها دارند را ترک نمی‌کنند. آن‌ها با رایانه، نامه و تلفن‌های همراه با هم می توانند در ارتباط باشند و ممکن است از این تکنولوژی‌ها برای اذیت و آزار یکدیگر، قلدری کردن و آسیب رساندن به دیگران استفاده کنند.

۵ چگونه کاربران مزاحم را مسدود و مسائل را گزارش کنیم

شما می‌توانید تمام مکالمات صورت گرفته را در یک واژه پرداز کپی و جایگذاری کنید. بسیاری از نرم‌افزارهای گفتگوی آنلاین به شما اجازه می‌دهند تا با راست کلیک کردن بر روی نام کاربران در لیست دوستان‌تان آن‌ها را «مسدود» یا از آن‌ها «صرف‌نظر» کنید. اگر کودک شما در معرض یک تعرّض آنلاین قرار گرفته است، یک کپی از سابقه‌ی مکالمات را به مدیر اطاق گفتگو یا مدیر سایت ارسال کنید. شما می‌توانید اطّلاعات تماس را از بخش «کمک» یا بخش «گزارش‌دهی» برنامه دریافت کنید. همچنین در صورتی که موضوع از اهمیت خاص و ویژه‌ای برخوردار است، موضوع را از طریق «ثبت شکایت» در وب‌سایت پلیس فتا به آدرس www.cyberpolie.ir به پلیس اعلام کنید.

الفبای امنیت آنلاین
برای نوجوانان
۱۳ تا ۱۹ ساله‌ها

نوجوانان

پلیس فتای تولید و تبادل اطلاعات ناجا
CYBER POLICE

الف با نوجوانان خود صحبت کنید

همان‌طور که شما دوست دارید امنیت عبور و مرور را پیش از آن‌که آنان شروع به رانندگی کنند، به نوجوانان خود بیاموزید، همچنین باید در رابطه با امنیت اینترنت نیز، پیش از آن‌که به آنان اجازه دهید بدون نظارت شما در اینترنت گشت بزنند، آموزش دهید.

یک فرق عمده بین رانندگی و استفاده از اینترنت آن است که «قوانین عبور و مرور» واقعی در اینترنت وجود ندارد. به همین خاطر اینترنت، تبدیل به یک وسیله‌ی نقلیه قدرت‌مند و البته خطرناک شده‌است. بنابر این، برای کاستن از خطرات و آسیب‌های رایانه، شما بایستی قوانینی را تعریف کنید و به اجرا بگذارید. در این‌جا هدف نهایی، تربیت و آموزش حسّ مشترک نوجوانان برای درک روشن و شفّاف خطرات آنلاین است.

با نوجوانان خود صحبت کنید که چرا ضروری است که در فضای آنلاین ایمن باشند. مطمئن شوید که در طیّ این صحبت‌ها موارد ذیل را ذکر می‌کنید:

- بحث در باره‌ی ویروس‌ها، جاسوس‌افزارها و هکرها و اقداماتی که انجام می‌دهند.
- بحث در رابطه با شکارچی‌های آنلاین که دوست دارند توجّه نوجوانان برای صحبت‌کردن درباره‌ی خودشان را جلب کنند.
- تشریح کنید که به دلیل این که رایانه یک در باز به سمت اطّلاعات مهم شخصی شماست، ضروری است که در هنگام آنلاین شدن از امنیت لازم برخوردار باشید.
- بحث درباره‌ی این که سرقت هویّت چگونه اتّفاق می‌افتد.
- بحث در مورد این واقعیت که شما یا یک خبره‌ی رایانه (در صورتی که شما خبره نباشید) می‌توانید هرگونه اتّفاقی را که بر روی کامپیوتر می‌افتد، ردگیری کنید.
- صحبت در باره‌ی این که چگونه مجرمین می‌توانند کنترل رایانه‌ی شما را به دست بگیرند به نحوی که شما مجبور باشید، یک رایانه‌ی تازه بخرید.

ب به نوجوانان خود گوشزد کنید افرادی که به صورت آنلاین در اینترنت ملاقات می‌کنند، غریبه هستند.

مهم نیست که غالباً چگونه با آن‌ها چت می‌کنند و مهم نیست که آن‌ها فکر می‌کنند که مخاطب خود را می‌شناسند، مهم این است که بدانند افرادی که به صورت آنلاین آن‌ها را ملاقات می‌کنند، غریبه هستند. مردم راجع به این که حقیقتاً که هستند دروغ می‌گویند و «دوست» تازه‌ی نوجوان شما ممکن است در واقعیت یک مرد چهل ساله باشد که خود را در سنّ و سال نوجوان شما جا زده است.

ج پروفایل نوجوان خود را در سایت‌های شبکه‌های اجتماعی چک کنید

مطمئن شوید که نوجوانان شما، اطّلاعات زیادی درباره خودشان را در سایت‌هایی مثل فیس‌بوک، مای‌اسپیس و سایر سایت‌های شبکه‌های اجتماعی، ارسال نکنند. مطمئن شوید عکس‌هایی که در سایت ارسال می‌کنند، برانگیزاننده نباشد. به آن‌ها یادآوری کنید که اگر به دام شکارچی‌های اینترنتی بیفتند، عواقب و سوء پیشینه‌ی آن ممکن است خانواده و دوستان را شرمسار کرده، در پذیرش آنان در دانشگاه یا در استخدام آنان در سازمان‌ها و شرکت‌ها تاثیر داشته باشد.

الفبای امنیت آنلاین
برای تازه‌کاران
در هر سنّ و سال

تازه کاران

همسر شما، همکار شما، شریک شما، خانواده‌ی شما، بستگان سببی شما یا پدربزرگ‌ها و مادربزرگ‌های شما ممکن است به تازگی کار با رایانه و اینترنت را آغاز کرده باشند. ممکن است آن‌ها به اندازه‌ای که شما فکر می کنید زرنگ نباشند و ممکن است قربانی کلاهبرداری‌های آنلاین و حملات سایبری قرار بگیرند. به هر حال، به یک راهنمایی مختصر از شما نیاز دارند. گفتگوی شما درباره‌ی امنیت وب بایستی شامل موارد ذیل باشد:

الف ویروس‌ها، جاسوس‌افزارها و هکرها

اگر شما می‌خواهید تعریف این عبارات را پیدا کنید می‌توانید آن‌ها را به راحتی از طریق جستجوهای آنلاین در واژه‌نامه‌های تخصّصی یا سایت‌ها و وبلاگ های تخصّصی IT بیابید. مطالب ارزشمندی نیز در وب‌سایت پلیس فتا به آدرس www.cyberpolice.ir در دسترس شما قرار دارد.

ب خطرات سرقت هویّت و فیشینگ

فیشینگ: جعل مجرمانه وب‌سایت یا ایمیل یک شخص یا شرکت و یا سازمان قانونی برای سرقت رمز عبور و شماره کارت‌های بانکی است. ایده‌ی خوبی است که شما از خدمات آنلاین استفاده کنید، امّا باید مطمئن باشید که مدام وضعیت کارت بانکی و صورت حساب‌هایی که از سوی بانک صادر می شود را چک می‌کنید.

ج اهمیّت محتاط بودن در زمان دانلود آیتم‌های رایگان

به کسانی که دوست‌شان دارید یادآوری کنید که طبق ضرب‌المثل قدیمی هرچیزی قیمتی دارد، حتّی اگر رایگان باشد! بنابر این به آن‌ها هشدار دهید که اگر این نرم‌افزارها را دانلود کنند، ممکن استبا تبلیغ‌افزارها و جاسوس‌افزارها در آن برنامه مواجه شوند.

توافقنامه امنیت اینترنتی خانواده

توافقنامه‌ی پیش رو، قوانین فضای آنلاین خانه‌ی ما را ایجاد می‌کند. ما این توافقنامه را امضا کرده و در مقاطع زمانی منظّم متناسب با بزرگ‌شدن فرزندان‌مان آن را به روز می‌کنیم.

۱ – ما هرگز اطّلاعات شخصی خود مثل نام خانوادگی، آدرس منزل و شماره‌ی تلفن خود را به دیگران نمی‌دهیم. همچنین نام مدرسه، شهر، خواهر و برادرمان، تیم ورزشی و محل کار پدر و مادر را با کسی در میان نخواهیم گذاشت.

۲ – ما توافق می‌کنیم که کلمه‌ی عبور خود را به هیچ کسی خارج از دایره‌ی خانواده‌ی خود ندهیم. ما همه متفّق‌القول هستیم که با نام کاربری خود که والدین آن را می‌شناسند در اینترنت حضور داشته باشیم. ما تنظیمات رایانه و کلمه‌ی عبور خود را بی‌آن که از پدر و مادر اجازه داشته باشیم، تغییر نمی‌دهیم.

۳ – ما توافق می‌کنیم که زمان‌های آنلاین شدن خود را محدود کنیم به نحوی که تداخلی با سایر فعّالیّت‌های ما ایجاد نکند. ما توافق می‌کنیم که محدودیت زمانی ایجاد شده توسّط خانواده را رعایت کنیم و به اینترنت اجازه ندهیم که زمان انجام تکالیف منزل، ورزش و بازی و روابط رو در روی خانوادگی ما را بگیرد.

۴ – من هرگز با دوستان آنلاین در فضای واقعی ملاقات نخواهم کرد. همانطور که من در خیابان از غریبه‌ها پرهیز می کنم، از غریبه‌ها نیز در فضای اینترنت پرهیز می‌کنم. اگر کسی از من خواست تا با او در فضای واقعی دیدار داشته باشم، پدر و مادرم را سریعاً مطّلع خواهم کرد.

۵ – در صورتی که از چیزی احساس ناراحتی به من دست داد، من به آن‌ها واقعیت را گفته و دروغ نخواهم گفت. اگر کسی حرف‌های زشتی به من بزند یا کاری کند که من احساس ناراحتی کنم، من به سرعت از آن فضا خارج شده و به پدر و مادرم اطّلاع خواهم داد.

۶ – من هرگز صفحاتی که برای بزرگ‌سالان به وجود آمده‌است، را نخواهم دید. اگر این اتّفاق سهواً افتاد، از آن صفحه خارج شده و خانواده‌ام را آگاه خواهم کرد. من می‌دانم که تنها یک کلیک با سایت‌های بد فاصله دارم و این سایت‌ها هرگز برای کودکان مناسب نیستند.

۷ – من تنها با اجازه‌ی پدر و مادرم، عکس و فایل از اینترنت دانلود خواهم کرد. بعضی از این فایل‌ها ممکن است دارای عکس‌های نامناسب یا ویروس‌های خطرناک باشند که به رایانه‌ی من آسیب می‌رساند.

۸ – من هرگز عکس‌های خانوادگی یا شخصی خود را برای افراد آنلاین ارسال نمی‌کنم. تنها زمانی این کار را خواهم کرد که پدر و مادرم به من بگویند که کار درستی انجام می‌دهم.

۹ – من همیشه در امنیت خواهم بود. زیرا که قول می‌دهم این قوانین را حتّی وقتی که در خانه‌ی دوستانم، مدرسه یا در کتابخانه هستم رعایت کنم همانطور که در خانه آن‌ها را رعایت می‌کنم.

۱۰ – من می‌دانم که هیچ چیز بر روی اینترنت محرمانه نیست. من می‌پذیرم که پدر و مادرم می‌توانند ایمیل من را بخوانند یا وب‌سایت‌هایی را که از آن‌ها بازدید کرده‌ام،چک کنند. نه به خاطر این که آن‌ها به من اعتماد ندارند، بلکه به این خاطر که آن‌ها می‌خواهند مطمئن شوند که من در امنیت قرار دارم.

ما با موارد بالا موافقت می‌کنیم:

امضای فرزندان　　امضای پدر و مادر