شرکت مادر تخصصی تولید نیروی برق حرارتی
پژوهشگاه نیرو
برسام
برنامه‌سازمانی آگاهی‌رسانی امنیت سایبری
شرکت تولید نیروی برق حرارتی

خبرنامه امنیت سایبری

• شمـــاره اول • نیـمـه اول مـرداد ۱۴۰۱

گروه سابانجی **رادی‌فلو** را خرید

هشدار آمریکا درباره **بدافزار خطرناک** روی اسکادا

رفع آسیب‌پذیری‌های **یوکوگاوا**

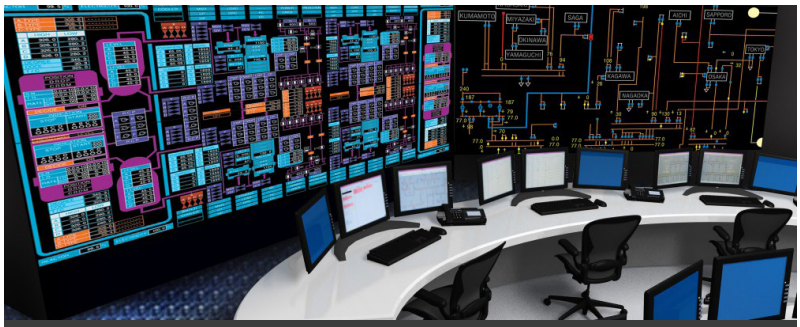
پنج روش کاهش آسیب باج‌افزارها به شبکه‌های صنعتی

من کی می‌توانم تلفن همراه داشته باشم؟

خبرنامه امنیت سایبری

نیمه اول مرداد ۱۴۰۱

فهرست



هشدار آمریکا درباره
بدافزار خطرناک روی اسکادا

چارچوب حمله ماژولار ICS به‌طورمعمول برای ایجاد اختلال و یا تخریب دستگاه‌های صنعتی قابل‌استفاده است.

دولت ایالات‌متحده پس از کشف ابزارهای سفارشی جدیدی که توانایی به‌خطر انداختن کامل سیستم و اختلال در دستگاه‌ها و سرورهای ICS/SCADA هستند، به‌شدت در خصوص این سو استفاده از این ابزارها هشدار داد.

گزارش مشترک ارگان‌های وزارت انرژی، NSA، CISA و FBI آمریکا خاطرنشان می‌کند که فعالان ناشناس APT ابزارهایی تخصصی ایجاد کرده‌اند که قادر به ایجاد صدمات جبران‌ناپذیر به PLCهای شرکت اشنایدر الکتریک و OMRON و سرورهای بنیاد منبع باز OPC هستند.

این سازمان‌ها در گزارش خود تأکید کردند این ابزارها مهاجمان را قادر می‌سازد دستگاه‌های قربانی را پس از دسترسی اولیه به شبکه فناوری عملیاتی (OT) اسکن کرده و در اختیار بگیرند. علاوه بر این، آنان قادر خواهند بود با استفاده از اکسپلویت درایور مادربرد ASRock که آسیب‌پذیری‌های معروفی دارند، به ایستگاه‌های کاری مهندسی مبتنی بر ویندوز موجود در محیط‌های فناوری اطلاعات (IT) یا فناوری عملیات (OT)، آسیب برسانند.

این هشدار دولتی در پی یک سری حملات بدافزاری پاک‌کننده (wiper malware) مرتبط با تهاجم روسیه به اوکراین و به خطر افتادن زنجیره تأمین نرم‌افزار صورت گرفت که در یک برهه زمانی سرویس اینترنت ماهواره‌ای Viasat را نیز به‌کلی از کار انداخت.

گروه سابانجی
رادی‌فلو را خرید

شرکت صنعتی و مالی Sabanci Group ترکیه قراردادی برای تصاحب اکثریت سهام شرکت امنیت سایبری فناوری عملیاتی Radiflow را به مبلغ ۴۵ میلیون دلار امضا کرد.

شرکت رادی‌فلو مستقر در سرزمین‌های اشغالی راه‌حل‌های امنیت سایبری را برای شبکه‌های زیرساختی حیاتی، ازجمله مدیریت ریسک، مشاهده و تشخیص ناهنجاری و محصولات دسترسی ایمن ارائه می‌کند.

سابانجی ترکیه بنا دارد در ابتدا ۵۱ درصد از سهام رادی فلو را به قیمت ۴۵ میلیون دلار خریداری کند و در مرحله بعد این شرکت را به‌طور کامل در سال ۲۰۲۵ تصاحب کند.

این خرید از طریق بخش خدمات فناورانه Investment BV ، یک شرکت سرمایه‌گذاری جدید متمرکز بر خدمات دیجیتال که توسط سابانجی در هلند تأسیس‌شده است، انجام خواهد شد.

ایلان بردا، مدیرعامل رادی‌فلو، در این خصوص گفت: «این خرید به ما امکان می‌دهد سبد راهکارهای خود را متنوع‌تر کنیم و جایگاهمان را در میان صنایع مهم تقویت کنیم. معتقدیم که این اقدام فاز بعدی در مدیریت ریسک ما بر اساس معیارهای این صنعت است. همکاری ما با شرکت‌های تابعه گروه سابانجی بینش عمیقی در مورد بخش‌های مختلف صنعتی به ما ارائه می‌دهد و قادرمان می‌سازد راه‌حل‌های پیشگامی به مشتریان خود ارائه دهیم.

مدیرعامل رادی‌فلو خاطرنشان کرد که معامله با سابانجی بر عملیات و تعاملات روزمره این شرکت با شرکا و مشتریانش تأثیری نخواهد داشت.

رفع آسیب‌پذیری‌های یوکوگاوا

یوکوگاوا غول اتوماسیون ژاپنی می‌گوید توانسته اخیراً مجموعه‌ای از آسیب‌پذیری‌ها را در محصولات سیستم کنترل اصلاح کند. به گفته محققان، این اکسپلویت‌ها برای اختلال یا دست‌کاری فرآیندهای فیزیکی قابل سوءاستفاده هستند.

محققان شرکت امنیت سایبری صنعتی دراگوس در مجموع ده آسیب‌پذیری را در سیستم کنترل توزیع‌شده CENTUM VP Yokogawa (DCS) و سرور Exaopc OPC برای سیستم‌های CENTUM کشف کرده‌اند. یوکوگاوا در مورد حفره‌های امنیتی در ژانویه و فوریه اطلاعاتی را منتشر کرده است. آژانس امنیت سایبری و امنیت زیرساخت ایالات‌متحده (CISA) نیز در این خصوص توصیه‌های خود را در اواخر مارس (اوایل فروردین‌ماه) منتشر کرد.

این آسیب‌پذیری‌ها عمدتاً مربوط به اعتبارنامه‌های هاردکد شده، پیمایش مسیر (path traversal)، تزریق فرمان (command injection)، هایجک DLL، اختیارات دسترسی نادرست و مصرف کنترل نشده منابع می‌شوند. این نقص‌ها، که به تعدادی از آنها درجه‌بندی «به‌شدت بالا» اختصاص داده‌شده است، برای دسترسی به داده‌ها، هشدارهای سرکوب (suppress alarms)، بازنویسی یا حذف فایل‌ها، اجرای دستورات دلخواه، خرابی سرورها، و افزایش دسترسی‌ها مورد سوءاستفاده قرار گیرند.

بهره‌برداری از برخی آسیب‌پذیری‌ها مستلزم دسترسی محلی به سیستم هدف است؛ درحالی‌که برخی دیگر را می‌توان با ارسال بسته‌های ساخته‌شده ویژه به نرم‌افزار مدیریت هشدار ادغام‌شده (CAMS) برای ایستگاه رابط انسانی (HIS یا HMI) مورداستفاده یا درواقع سوءاستفاده قرارداد.

پنج روش کاهش آسیب باج‌افزارها به شبکه‌های صنعتی

در یک سال و نیم اخیر، شاهد افزایش بی‌سابقه حملات باج‌افزاری به شبکه‌های صنعتی فناوری عملیاتی (OT) بوده‌ایم. حقیقتش این است این موضوع بیشتر برای مطبوعات تازگی دارد؛ درحالی‌که امری بود که کارشناسان صنعت از مدت‌ها قبل پیش‌بینی‌اش را می‌کردند. درواقع در همایش RSAC ۲۰۱۸ موضوع باج‌افزارها و حملات مخربشان برای تعدادی از مسئولان امنیتی بخش دولتی و خصوصی ارائه شده بود.

در چند مدت اخیر، شواهدی مبنی بر اینکه بازیگران دولتی نیز شبکه‌های OT را هدف قرار می‌دهند، آشکارشده است. اما در سال ۲۰۱۷، NotPetya به دنیا نشان داد که سرریز تصادفی باج‌افزار به شبکه‌های OT می‌تواند عواقب فاجعه‌باری داشته باشد. آن هنگام، عملیات روزمره شرکت‌های بزرگ متعددی، در بخش‌های وسیعی ازجمله مراقبت‌های بهداشتی، انرژی و حمل‌ونقل متوقف شد و حدود ۱۰ میلیارد دلار خسارت به بار آمد. برای مجرمان سایبری فقط مسئله زمان بود تا متوجه شوند که شبکه‌های OT برای عملیات شرکت‌ها حیاتی هستند و بنابراین بسیار ارزشمند محسوب می‌شوند.

راه‌اندازی شبکه‌های OT منتج به ایجاد درآمد و بهبود عملکرد مشتریان می‌شود. اگر حملات باج‌افزاری به‌طور خاص محیط‌های صنعتی را هدف قرار دهند، امکان از دست دادن دسترسی به آن هم هست. امری که بی‌شک بر کسب‌وکار اصلی شرکت تأثیر می‌گذارد. حتی از دست دادن نسبی نظارت اپراتورهای انسانی نسبت به فعالیت‌های شبکه، باعث می‌شود به خاطر کیفیت محصول یا دغدغه‌های ایمنی، فرآیند متوقف شود. درنهایت، هرگونه خطر اختلال در فرآیندهای فیزیکی می‌تواند منجر به خسران و زیان در بهره‌وری و درآمد شود یا حتی در برخی موارد موجب به خطر افتادن جان انسان‌ها شود.

در فهرست هشدارهای دولتی، برخی تاکتیک‌ها و تکنیک‌های متداول که هکرها برای نفوذ به سازمان‌ها استفاده می‌کنند، ذکرشده است. ازجمله spearphishing برای دسترسی به شبکه IT و سپس پیووت کردن به شبکه OT؛ یا اتصال مستقیم به کنترل‌کننده‌های با قابلیت دسترسی به اینترنت که نیازی به احراز هویت کاربر یا دستگاه ندارند. از این مرحله به بعد،

شرایط برای استقرار باج‌افزار و رمزگذاری داده‌ها مهیاست. در بسیاری از موارد، به دلیل تعداد محدود کنترل‌های امنیتی در شبکه‌ها، نفوذکننده می‌تواند ماه‌ها یا حتی سال‌ها از شبکه OT عبور کند؛ بدون اینکه کسی متوجه شود.

اخیراً، آژانس‌های دولتی آمریکا اذعان کردند که BlackMatter درواقع نوعی تغییر نام تجاری احتمالی DarkSide است، گروهی که به Colonial Pipeline حمله کرد و از آن زمان چندین نهاد زیرساختی حیاتی ایالات‌متحده، ازجمله دو مورد در بخش غذا و کشاورزی را هدف قرار داده است. چه این کار یک تغییر نام باشد و چه آن‌طور که برخی کارشناسان امنیتی استدلال می‌کنند، انشعاب باشد، ظاهرا این گروه از بازیگران دولت_ملت به دنبال این هستند تا با اختلال در دسترسی مصرف‌کنندگان به خدمات زیرساختی حیاتی، اقتصاد و زندگی روزمره میلیون‌ها نفر را مختل کنند.

با سرعتی که روندهای تحول دیجیتال و دور کاری می‌پیماید، می‌توان گفت زیرساخت‌ها بیش از هر زمان دیگری تحت‌فشار قرارگرفته‌اند. قبلاً حملات به زیرساخت‌ها قریب‌الوقوع بود، اما اکنون قابل‌لمس است. ولی هنوز مرحله آخر باقی می‌ماند، زیرا امروزه شبکه‌های OT به‌طور فزاینده‌ای به زیرساخت‌های فناوری اطلاعات متصل می‌شوند. با توجه به لزوم افزایش بهره‌وری و سودآوری کسب‌وکارها، شرکت‌ها از اتصال بیش‌ازحد (hyperconnectivity) استقبال کردند - که البته چیز بدی نیست. اما اکنون الزام و فوریت اصلی این است که این اتصال‌ها امن‌تر شود.

با توجه به این شرایط جدید، شرکت‌ها چه‌کاری می‌توانند برای تقویت وضعیت امنیتی محیط‌های OT خود انجام دهند؟ باهم پنج توصیه را مرور می‌کنیم که هر CISO (مسئول ارشد امنیت اطلاعات) باید در نظر بگیرد:

۱. دامنه حاکمیت ریسک (risk governance) خود را گسترش دهید

تا هر چیزی را که دارایی فیزیکی-سایبری است پوشش دهد. این دامنه شامل تمام مؤلفه‌های اینترنت اشیاء صنعتی (Industrial IoT)، سیستم کنترل صنعتی (ICS) و مؤلفه‌های اینترنت اشیاء سازمانی (Enterprise IoT) می‌شود. البته، همین کار یک گام چالش‌برانگیز برای بسیاری از سازمان‌ها به‌حساب می‌آید؛ زیرا حتی شناسایی این دارایی‌ها کار آسانی نیست. ممکن است لازم شود این فرآیند چندین بار تکرار شود. خوشبختانه، در چند سال اخیر صنعت دنیا پیشرفت چشمگیری در فناوری داشته است که به ما کمک می‌کند چنین دارایی‌هایی را به‌راحتی کشف کنیم و میزان مواجهه، ریسک و آسیب‌پذیری‌های آنها را مشخص کنیم.

۲. مطمئن شوید که بین شبکه‌های IT و OT تقسیم‌بندی مناسبی دارید

فرآیندها و برنامه‌های تجاری زیادی وجود دارد که باید در سراسر مرز IT/OT با یکدیگر ارتباط برقرار کنند، بنابراین باید اطمینان حاصل کنیم که این کار به روشی امن انجام می‌شود. این گام ساده معمولاً بدیهی تلقی می‌شود، اما نباید این‌طور باشد. علاوه بر بخش‌بندی IT/OT، تقسیم‌بندی مجازی در خود مناطق درون محیط OT را هم مدنظر داشته باشید- این کار به تشخیص حرکت‌های جانبی (lateral movement) در شبکه‌های OT کمک می‌کند- و اگر عملیات از راه دور نیاز به دسترسی مستقیم به شبکه‌های OT دارد، مطمئن شوید که این کار از طریق یک اتصال دسترسی از راه دور ایمن با کنترل‌های دقیق روی کاربران، دستگاه‌ها و نشست‌ها انجام می‌شود.

۳. اصول امنیت سایبری را رعایت کنید

اطمینان حاصل کنید که امنیت سایبری شما به دستگاه‌های OT و IoT نیز گسترش می‌یابد. این امر شامل استفاده از گذرواژه‌های قوی (و به اشتراک نگذاشتن گذرواژه‌ها در بین کاربران مختلف، عملی که در محیط‌های صنعتی رایج است)، مخزن رمز عبور و احراز هویت چندعاملی است. برخی از فرآیندها، مانند اصلاح سیستم‌های قدیمی، ممکن است چالش‌برانگیزتر باشند یا حتی اصلاً امکان‌پذیر نباشند. اگر چنین است، کنترل‌های جبرانی مانند فایروال و لیست‌های کنترل دسترسی را تعریف و اجرا کنید. آژانس امنیت سایبری و امنیت زیرساخت (CISA) دارای تعدادی ابزار امنیت سایبری بدون هزینه است؛ ازجمله اسکن و آزمایش برای کمک به کاهش امکان قرار گرفتن در معرض تهدیدات.

۴. یک برنامه نظارت بر سیستم خوب و قوی را اجرا کنید

این کار به معنای نظارت بر تهدیدات در شبکه‌های IT و OT و هر چیزی است که از آن محدوده عبور می‌کند. راه‌حل‌های بدون عامل یا به‌اصطلاح agent-less، که برای نظارت مستمر بر تهدیدها در سراسر شبکه OT ساخته‌شده‌اند، می‌توانند به‌سرعت پیاده‌سازی شوند، به‌خوبی با سیستم‌ها و گردش‌های کاری OT و IT ادغام شوند و به تیم‌های IT و OT اجازه دهند تا محیط‌های OT را باهم ببینند. این تیم‌ها با استفاده از مجموعه‌ای از اطلاعات یکسان، گام‌های خاصی را برای مدیریت و کاهش ریسک ناشی از تهدیدات نوظهور شناخته‌شده و ناشناخته برمی‌دارند.

۵. تمرینات مرتبطی را در برنامه پاسخگویی به حوادث بگنجانید

اجرای تمرینات مقابله با حملات باج‌افزار به شما در درک آمادگی سازمانی و فنی‌تان کمک خواهد کرد. این کار به شما فرصتی می‌دهد تا یک برنامه واکنش بهبودیافته ترتیب دهید و باعث افزایش اعتمادبه‌نفستان در خصوص آمادگی و انعطاف‌پذیری در برابر چنین حملاتی می‌شود.

حملات باج‌افزاری خطوط پردازش و توزیع کارخانه‌ها را مختل می‌کنند. اگرچه به نظر می‌رسد هیچ‌یک از این حملات مستقیماً بر محیط OT تأثیری نداشته است، موضوع فقط زمان است. با انجام چند قدم ساده و اساسی می‌توانید خطر باج‌افزار را در محیط‌های صنعتی خود کاهش دهید.

من کی می‌توانم تلفن همراه داشته باشم؟

راهنمایی‌هایی در مورد اینکه چه زمانی تلفن همراه در اختیار کودکان بگذاریم

در دنیای کنونی ما، تصور زندگی بدون تلفن همراه سخت است. ما از تلفن همراه برای ارسال ایمیل‌های دورکاری، ایجاد لیست‌های خرید مواد غذایی، عکس گرفتن، تبادل پیام‌های کاری و دوستانه و حتی پرداخت قبوض و انجام کارهای بانکی روزانه خود استفاده می‌کنیم. اما به‌عنوان والدین، یک سؤال دراین‌بین پیش می‌آید: فرزند ما چه زمانی باید صاحب تلفن همراه شود؟

۱. تلفن‌های همراه و فرزندان

به دلایل مختلفی والدین تصمیم می‌گیرند تلفن همراه در اختیار فرزندانشان قرار دهند ازجمله:

- فرزندان از آن‌ها می‌خواهند که اجازه داشته باشند با دوستان خود ارتباط برقرار کنند.
- در تماس بودن با آنها در طول روز و امکان دسترسی فوری در مواقع اضطراری
- سایر بچه‌های مدرسه تلفن همراه دارند و والدین نمی‌خواهند کودکشان در اجتماع منزوی باشد.
- برای استفاده از برنامه‌های آموزشی و بازی‌ها.
- تشویق به مسئولیت‌پذیری.

باوجوداینکه تلفن‌های هوشمند در زندگی روزمره ما ریشه دوانده‌اند، اما همان‌طور که این آمار نشان می‌دهد، جنبه تاریکی نیز با خود به همراه دارند:

- به‌طور متوسط، کاربران تلفن همراه هرروز ۲۶۱۷ بار از انگشت خود برای کلیک، ضربه و کشیدن صفحه تلفن استفاده می‌کنند.
- استفاده از تلفن همراه مقصر ۲۶ درصد تصادفات رانندگی است.
- ۴۵ درصد از نوجوانان احساس می‌کنند به گوشی‌های هوشمند خود معتاد شده‌اند.

آیا جای تعجب است که وقتی فرزند شروع به درخواست تلفن همراه می‌کند، والدین در مورد زمان انجام این کار ملاحظات و دقت بیشتری به خرج دهند؟ علیرغم خطرات ذاتی استفاده از گوشی‌های هوشمند، والدین می‌توانند به کودکان خود برای مستقل‌تر شدن و بهبود مهارت‌های اجتماعی کمک کنند تا بتوانند با آرامش خاطر در تماس منظم با فرزندان باشند.

۲. عوامل مهم پیرامون تلفن‌های همراه و فرزندان

تصمیم‌گیری در مورد زمانی که یک کودک باید گوشی هوشمند داشته باشد کاملاً شخصی و فردی است، اما بسیاری از کودکان در زمان مدرسه ابتدایی شروع به درخواست (و دریافت آن) می‌کنند. اگر دوستان و دانش‌آموزان دیگر در سنین پایین تلفن همراه داشته باشند، سایر کودکان نیز به‌احتمال‌زیاد از آنها تبعیت می‌کنند. بسیاری از کارشناسان معتقدند که هیچ سن جادویی برای استفاده از تلفن همراه وجود ندارد. والدین به‌جای اینکه فقط بر سن فرزند متمرکز باشند، باید چندین عامل دیگر را در نظر بگیرند.

۳. سطح بلوغ فرزند شما

هر کودکی با دیگری متفاوت است، بنابراین این سؤال پیش می‌آید که آیا فرزند شما به لحاظ عاطفی و روانی آمادگی داشتن تلفن همراه را داراست؟ آیا قادرند وسوسه‌های خود را کنترل کنند؟ آیا در مورد نشانه‌های اجتماعی آگاهی دارند؟ اگر آنها با شناسایی و درک نشانه‌های اجتماعی در زندگی غیرمجازی مشکل داشته باشند، توانایی آنها برای درک همین نشانه‌ها در یک محیط مجازی ممکن است با مشکل مواجه شود.

۴. رابطه شما با فرزندتان

خرید اولین تلفن همراه برای فرزندتان یک حرکت بزرگ است. دنیای کاملاً جدیدی از اطلاعات و دسترسی به آنها را پیش رویشان قرار می‌دهد. آیا می‌توانید مطمئن باشید که فرزندتان در مورد تعاملات مجازی خود با شما صادق باشد؟ اگر آنها قربانی آزار و اذیت سایبری شوند، آیا این مسئله را با شما در میان می‌گذارند و اجازه می‌دهند تا برای رفع مشکل کمکشان کنید؟ اگر کسی بخواهد او را وادار به انجام کاری نامناسب کند، آیا شما را در جریان قرار می‌دهد؟ قبلاً در خارج از قلمرو دیجیتال، چنین سناریوهای مشابهی چگونه مدیریت می‌شدند؟

۵. ملاحظات مالی

فرض بر این است قبل از اینکه فرزندتان شغلی داشته باشد شما یک تلفن همراه

برای او می‌خرید و علاوه بر هزینه گوشی، قبض ماهانه تلفن او را نیز پرداخت می‌کنید. بااین‌حال، ممکن است فرصتی به وجود آید که آنها از طریق پول‌توجیبی خود یا در ازای انجام کارهای خانه در پرداخت هزینه تلفن مشارکت کنند. هزینه‌های اینترنت و هزینه خرید برنامه‌ها و خریدهای درون برنامه‌ای چیزهایی هستند که باید قبل از خرید تلفن در مورد آنها توافق شود.

۶. عکس گرفتن

تلفن همراه دیگر فقط یک تلفن نیست. بلکه یک رایانه کاملاً کاربردی با زنگ‌ها و برنامه‌ها و ازجمله یک دوربین است. آیا می‌توانید به فرزندتان اعتماد کنید که با دوربینی که در دست دارد همیشه محتاطانه عمل کند؟ آیا عزت‌نفس آنها به‌اندازه کافی قوی است که از خطرات فرهنگ سلفی در امان بمانند؟ دوربین‌ها برای ثبت خاطرات و ابراز خلاقیت عالی هستند، به شرطی که از این ابزار به شیوه‌ای سالم و مناسب استفاده شود.

۷. چگونه در کمال آرامش خاطر و ایمنی از تلفن همراه استفاده کنیم

زمانی که از خود پرسیدید: چه زمانی باید به فرزندم تلفن همراه بدهم؟ و در مورد زمان انجام آن به نتیجه رسیدید به این توصیه کارشناسان توجه کنید که می‌گویند باید قراردادی بین والدین و فرزند گذاشته شودکه تأکید می‌کند تلفن همراه یک امتیاز است، نه یک حق و می‌توان آن را در هرزمانی و به هر دلیلی از کودک سلب کرد.

عناصر رایج این نوع قرارداد عبارت‌اند از دستورالعمل‌های مبتنی بر سن در مورد محدودیت‌های زمانی یعنی زمانی که آنها می‌توانند از تلفن استفاده کنند؛ ممنوعیت استفاده قبل از رفتن به رختخواب، سر میز شام یا در حین انجام تکالیف، نحوه استفاده از آن، قوانین برای گم‌شدن یا آسیب دیدن دستگاه و قوانین نظارت بر جستجوها و دانلودها.

در مسئله امنیت، ۸۸ درصد والدین رمز عبور تلفن همراه فرزندان خود را می‌دانند و اکیداً توصیه می‌شود هر والدینی که به فرزند خود تلفن همراه می‌دهد رمز عبور آن را بداند تا از آن برای بررسی دوره‌ای و نظارت بر نحوه استفاده از تلفن استفاده کند. این منبع به والدین کمک می‌کند تا اصطلاحات و زبان عامیانه اینترنتی در حال تکاملی که توسط نوجوانان استفاده می‌شود را بررسی کنند تا آنچه را که می‌خوانند درک کنند.

و درنهایت، بهترین گامی که والدین می‌توانند برای اطمینان از ایمنی فرزندشان در دنیای فناوری بردارند، استفاده از ابزارهای فناوری است. این ابزارهای فناوری مجهز به عملکردهایی مناسب خانواده مانند مدیریت پیشرفته گوشی توسط والدین، مسدودکننده‌های سایت بزرگسالان، مدیریت زمان روشن بودن گوشی، مکان‌یاب GPS است.

گوشی‌های هوشمند می‌توانند بسیار مفید باشند. یافتن راه‌هایی برای معرفی ایمن آنها به دنیای فرزندتان به‌عنوان یک دارایی و منبع واقعی که مستلزم صداقت و مسئولیت‌پذیری است، به آنها کمک می‌کند تا از این فناوری به شیوه‌ای سالم و سازنده استقبال کنند.

کارگروه فرهنگ‌سازی و آگاهی‌رسانی امنیت سایبری
شرکت مادرتخصصی تولید نیروی برق حرارتی (برسام)

تلفن دبیرخانه کارگروه برسام : **۵۸۳۷۶۶۴۲**

پست الکترونیکی کارگروه برسام : **Barsam[at]tpph.ir**