امنیت اطلاعات
امنیت سایبری
(Cyber Security)

چرا واقعا مهم است؟
کجا کاربرد دارد؟
چگونه به ما کمک می‌کند؟

در دنیای امروز،

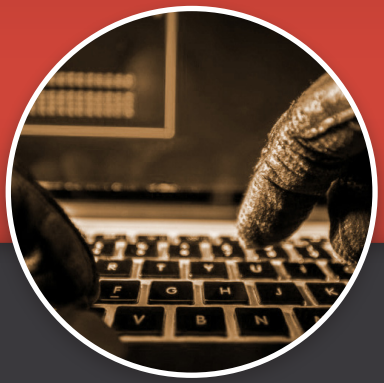
حفظ امنیت سایبری

دیگر یک انتخاب نیست،

یک الزام است.

درباره چیزهایی که خواندید، اگرسوالی داشتید؛ نه تنها خوشحال می‌شویم که بشنویم و پاسخ دهیم، بلکه شما را تشویق می‌کنیم که بیشتر کنجکاوی کنید و بیشتر سوال کنید!

تلفن مرکز: ۵۸۳۷۶۶۴۲ ایمیل مرکز: Barsam(at)tpph.ir



امنیت سایبری
به چه کسی مربوط است؟

اگر از شما سوال کنند که امنیت منزل شما به چه کسی مربوط است؛ پاسخ خواهید داد اول به خودم و بعد به پلیس و بعد به بقیه نهادهای مرتبط. چه خوب است اگر در امنیت اطلاعات هم همین رویکرد را داشته باشیم. درست است که اداره، سازمان، محل کار، بانک، شبکه اجتماعی و بقیه باید خودشان مراقب امنیت خدمات‌شان باشند اما شما هم مسئول حفظ امنیت خودتان هستید. در واقع این حفظ امنیت زنجیره‌ای است که همه‌مان بخشی از آن هستیم و هرکجا که نقصی در آن وارد شود، باعث ضربه‌خوردن بقیه هم می‌شود.

به این حقیقت توجه کنیم که مهم‌ترین چالش ارتباطات، موضوع «اعتماد» است و این همان نقطه آسیب‌پذیر همه ماست. بدانیدکه اکثر وب‌سایت‌ها به‌شدت مشتاق هستند تا هم برای شخصی‌سازی سرویس‌ها و هم نشان دادن تبلیغات، تا حد ممکن اطلاعات بیشتری درباره شما ذخیره کنند، با این بهانه که دفعه بعدی که به آن وب‌سایت سر می‌زنید، دردسر ورود مجدد اطلاعات یا خواسته‌هایتان را نداشته باشید. این نشان می‌دهد که بیش از آنچه که فکر می‌کنید، اطلاعات شما در اینترنت ذخیره شده و موجود است. حالا کافی است که این اطلاعات به نحوی با اطلاعات کارت بانکی یا سایر علایق شما ترکیب شود تا ارزش آن اطلاعات چند برابر شود.

این اطلاعات ارزشمند دقیقا همان چیزهایی هستند که توجه هکرها را به کامپیوترها یا تلفن‌های همراه جلب می‌کند. و این پاسخ سوال همان افرادی است که می‌گویند کامپیوتر یا تلفن من چیزی ندارد که هکرها به آن علاقمند باشند. پس بیایید در زنجیره تامین امنیت اطلاعات، شما ضعیف‌ترین حلقه نباشید!

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

چرا امنیت ؟

آیا امنیت سایبری موضوعی ناخوشایند و دست‌وپاگیر است؟ آیا حفظ امنیت اطلاعات فقط به متولیان آن مربوط می‌شود یا همه درگیر آن هستند؟ آیا علاقه‌ای به پرسیدن سوالات مربوط به امنیت سایبری ندارید؟

خب اجازه دهید اول از محیط کار شروع کنیم. در محیط کاری‌مان چه چیزهایی به امنیت اطلاعات و امنیت سایبری مربوط می‌شود؟

رمزهای عبور، کنترل ورود و خروج به مراکز مهم، حساسیت درباره ایمیل‌های دریافتی، عدم انتشار اطلاعات «حساس، شخصی یا خاص» در فضای مجازی و پیام‌رسان‌ها، توجه به تنظیمات آنتی‌ویروس و ابزارهای حفاظتی، آشنایی با روش‌های فریب و مهندسی اجتماعی، الزامات به همراه آوردن تجهیزات شخصی مانند لپ‌تاپ و اتصال آن به شبکه سازمانی و مسائلی از این دست را می‌توان در حوزه امنیت سایبری دسته‌بندی کرد.

اما آیا می‌توان با شعار حفظ اطلاعات از همه این امکانات چشم‌پوشی کرد؟ قطعا خیر و منظور از امنیت اطلاعات، افزایش قفل و بند و محدودکردن همه چیز نیست؛ منظور هشیاری در نحوه کنترل سامانه‌ها و حفظ اطلاعات یا همان دارایی‌های دیجیتالی سازمان است.

یعنی با داشتن **آگاهی، شناخت و تبعیت** از سیاست‌های امنیت اطلاعات سازمان و توجه به **حفظ دارایی‌های دیجیتالی** **سازمان** می‌توان به‌عنوان یکی از حلقه‌های زنجیر تامین امنیت عملکرد خوبی داشت.

همه آگاهیم که بسیاری از مشکلات امنیتی که در فناوری اطلاعات بروز می‌کند، غیرعمدی و فقط از روی سهل‌انگاری یا گاهی خیرخواهی نابجا است. به همین دلیل است که می‌گویند **قدرت یک زنجیر معادل قدرت ضعیف‌ترین حلقه آن است** و ضعیف‌ترین حلقه زنجیر امنیت سایبری، نیروی انسانی است! پس با اهمیتی که این موضوع دارد، ما نباید ضعیف‌ترین حلقه زنجیر باشیم.

امنیت در عملیات بانکی آنلاین

تا چند سال قبل، بانک‌ها خدمات خود را به دو بخش بانکداری متعارف و بانکداری الکترونیکی تقسیم‌بندی می‌کردند. اما امروزه این تقسیم معنای خود را از دست داده است. احتمالا همین امروز هم شما یک عملیات بانکی را از طریق تلفن همراهتان یا کامپیوترتان انجام داده‌اید. اینکه بانک یا طرف گیرنده پول از شما چه فرآیندهایی را برای امن‌سازی خدمات خود انجام داده، یک بحث است و اینکه شما برای حفظ اطلاعات مهم‌تان چه کارهای امنیتی را انجام می‌دهید؛ موضوعی دیگر.

پس در مقابل آسانی، ارزانی و سرعتی که این خدمات برایمان به ارمغان آورده، لازم است که نکاتی را رعایت کنیم. این موارد که اتفاقا خیلی هم پیچیده نیستند، می‌توانند تا حد زیادی مانع از بروز مشکلات شوند.

کارهایی مانند توجه به **آدرس دقیق** سایت اینترنتی که می‌خواهیم از طریق آن پرداخت را انجام دهیم، تا در دام چیزی که به آن **فیشینگ** می‌گویند نیفتیم؛ عدم توجه به پیام‌ها و تماس‌هایی که ما را برای دریافت جایزه و هدیه به آمدن به پای **خودپرداز** دعوت می‌کنند، **حفظ رمز** کارت بانکی و استفاده نکردن از رمزهای بسیار ساده، توجه نکردن به پیام‌هایی که ما را به نصب نرم‌افزار تشویق می‌کنند، استفاده از **آنتی ویروس** روی دستگاه‌هایی که با آن‌ها پرداخت انجام می‌دهیم، عدم استفاده از **اپ‌های متفرقه** یا ناشناس که وعده‌های عجیب و غریب می‌دهند، کلیک‌نکردن روی لینک‌هایی که وعده فروش شارژ با **جوایز میلیاردی** می‌دهند، ارسال نکردن **تصویر کارت** بانکی‌تان حتی برای دوستان و نزدیکان می‌تواند امنیت شما را تا حد بسیار خوبی افزایش دهد.

شبکه‌های اجتماعی

آیا حفظ «امنیت سایبری» فقط مربوط به سازمان و اداره و محل کار است یا در خانه و مدرسه و جامعه هم باید درباره آن بدانیم و کنجکاوی کنیم؟ بدیهی است که حفظ امنیت سایبری در همه جا اهمیت دارد، اما چگونه می‌توان به آن دست یافت؟

مهم‌ترین نکته آن است که همان‌طوری که در فضای واقعی، بدون دلیل به کسی اعتماد نمی‌کنیم، در فضای مجازی هم نباید به ناشناس‌ها اعتماد کنیم؛ خصوصا در شبکه‌های اجتماعی. مطمئن باشیم که هیچ‌کس بدون دلیل نه به ما هدیه‌ای می‌دهد و نه برای یک خرید اندک، قرار است جوایز کلان به دست بیاوریم و نه بدون اطلاع ما قرعه‌کشی‌هایی انجام شده که برنده آن شده باشیم!

به علاوه مهم است بدانیم که تقریبا هر چیزی که روی اینترنت و شبکه‌های اجتماعی می‌فرستیم، محرمانگی خود را از دست می‌دهد و باید فرض کنیم که همه به آن دسترسی دارند!

تغییر نگرش سخت است ولی بدانید همه چیزهای محرمانه‌ای که شما از روی نیت خوب برای دوست یا همکارتان می‌فرستید، ممکن است به سادگی با هک شدن دستگاه دوست یا همکارتان لو برود ... و شما می‌مانید و شرمندگی و عواقب اتفاقی که نقشی مستقیم در بروز آن نداشته‌اید.

پس اطلاعاتی که ارسال می‌کنید را محدود کنید، از رمزهای عبور قوی استفاده کنید، به ناشناس‌ها هرگز اعتماد نکنید و شکاک باشید، برنامه‌هایتان را مرتب بروز کنید، و در آخر اینکه هرکجا که شک کردید، از متخصصان سوال کنید.