افتای ایرانی
در سالی که گذشت

نوروز ۱۳۹۳ www.aftana.ir

ویژه‌نامه خبری افتانا

بررسی وضعیت امنیت فضای تولید و تبادل اطلاعات در سال ۱۳۹۲ در گفتگو با کارشناسان

به همراه راهنمای تصویری انواع حملات فیشینگ

دیده‌بان
امنیت فناوری اطلاعات

بسم الله الرحمن الرحیم

دیده‌بان ۶
امنیت فناوری اطلاعات

افتای ایرانی در سالی که گذشت
ویژه‌نامه نوروزی افتانا
اسفند ۱۳۹۲/ فروردین ۱۳۹۳

سردبیر: علیرضا صالحی
گفتگوها: مریم اصلان زاده
گرافیک: ارشاد نیک‌خواه
با سپاس از: شرکت‌های شاپرک، ارتباط امن، پویه، ایمن رایانه پندار، توسن، تجارت امن، امن افزار گستر شریف، آیکو، بیت دیفندر.

info@aftana.ir تلفن: ۸۸۵۱۹۱۸۲

پایگاه خبری افتانا

افتا، چیزی از جنس فرهنگ است

علیرضا صالحی

با انتشار ابلاغیه مقام معظم رهبری در خصوص سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات (افتا)، فصل جدیدی در توجه و تمرکز بر این موضوع در فضای آی‌تی کشور گشوده شد.

در بند نخست این ابلاغیه به «ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای ایمن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات» اشاره شده است و بلافاصله در ادامه آن آمده است که ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی» مورد نظر است.

اما این امن‌سازی ناظر به «استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور، حفظ فرهنگ و هویت اسلامی-ایرانی و ارزشهای اخلاقی و حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی» خواهد بود. دیده می‌شود که منظور از امنیت فضای تولید و تبادل اطلاعات، فراهم آوردن امکانات، اندیشیدن تدابیر و آماده‌سازی زیرساخت‌هایی است که در آن مواردی چون عدم بروز اختلال در سرویس‌ها و خدمات عمومی یا پاسداری از حریم خصوصی و سرمایه‌های مادی و معنوی، از جمله موارد مهم برشمرده شده است.

در اندیشیدن به این بایسته‌ها، می‌بینیم که در بندی دیگر ابلاغیه به یکی از بنیادی‌ترین نکته‌ها یعنی فرهنگ‌سازی و آموزش پرداخته شده است. در بند هشتم آمده است که «فرهنگ‌سازی، آموزش و افزایش آگاهی و مهارت‌های عمومی در حوزه افتا» باید مورد توجه واقع شود یعنی باید دانست که «افتا» چیزی است از جنس بسترسازی، فرهنگ‌سازی و رفع دغدغه‌ها برای فراهم‌سازی امکان فعالیت ایمن و پایدار.

اما فضای تولید و تبادل اطلاعات را اغلب به دفاع سایبری مرتبط می‌دانند. بسیاری بر این تصور هستند که وقتی از افتا صحبت می‌کنیم، در ادامه باید به حملات سایبری، لزوم توجه به دفاع در این حوزه و داشتن استراتژی دفاعی بپردازیم. حال آنکه همانگونه که گفته شد، در ابلاغیه رهبر معظم انقلاب به موارد دیگری نیز اشاره شده که می‌توان نقاط بسیار مهم دیگری از جمله ایجاد زمینه‌های توسعه فناوری‌های بومی، توجه به حفظ حقوق فردی و اجتماعی افراد، حفظ فرهنگ و هویت اسلامی- ایرانی و ... را نیز در آن دید.

از همین رو به نظر می‌آید که در کشور بیش از آنکه نیازمند توجه و تدوین راهکار یا راهبرد باشیم، باید به سیاست‌گذاری کلان بیندیشیم. در همین راستا، خوشبختانه در مراجعه به سند راهبردی افتای کشور (مصوب اسفندماه ۱۳۸۷) می‌بینیم که در مقدمه آن به روشنی به چنین مواردی اشاره شده است:

- امنیت فضای تولید و تبادل اطلاعات مفهومی کلان و میان رشته‌ای است که بر مفاهیم و نظریات گوناگونی در حوزه‌های مختلف دانش مبتنی است.
- امنیت فضای تولید و تبادل اطلاعات امری نسبی است که به تلقی از مفهوم امنیت، کارایی و هزینه وابسته است.
- امنیت فضای تولید و تبادل اطلاعات امری زمینه‌وند است و مجموعه آداب و سنن، اخلاقیات، قوانین و سایر مقولات اجتماعی در آن تأثیر دارد.
- امنیت فضای تولید و تبادل اطلاعات به مرزهای جغرافیایی محدود نمی شود و از حوزه‌های داخلی، منطقه‌ای و جهانی تأثیر می‌پذیرد.
- حوزه تأثیر امنیت فضای تولید و تبادل اطلاعات، کلیه فعالیت‌های آحاد جامعه در این فضا را شامل می‌شود.

آنچه که باید در حوزه افتا رخ دهد، گوناگون و چند وجهی است. همانگونه که در سند افتا هم آمده، میان رشته‌ای و زمینه‌وند.

متولیان متعدد، اهداف و آمال گوناگون و ماموریت‌ها و وظایف متضاد و متعارض گاهی. برآمدن دولت تدبیر و امید، امیدوارمان کرده که در افتا، به دور از امنیتی شدن، به امن‌شدن بیندیشیم و جنبه‌های مختلف آن را واکاوی کنیم.

* این یادداشت قبلاً در مرجع امنیت (۱۳۹۲) منتشر شده و افتانا آن را بازنشر می‌نماید.

بروزرسانی امنیت در شاپرک

انتها نخواهد داشت

تامین امنیت در شبکه‌های بانکی و نظام پرداخت با توجه به سطح بالای تراکنش‌ها و معاملات مالی همواره یکی از مهمترین موضوعات در نظام بانکی است که راه اندازی مرکز شاپرک خود مبین این مسئله است گفتگویی داشتیم با سامان قطبی مدیر عامل شاپرک و مهندس آزادی مدیر کارگروه امنیت شرکت‌های PSP شاپرک که شرح آن را در ادامه می‌خوانید.

لطفا بفرمایید دلیل راه اندازی مرکز شاپرک چیست؟

قطبی: سیستم شاپرک حدود یک و سال و نیم است که راه اندازی شده است، با سرعت بالایی که رشد تکنولوژی و راه اندازی، توسعه و عملیاتی شدن بانکداری الکترونیک و خدمات مبتنی بر کارت داشته اند با توجه به چارچوب‌های مورد نیاز رشد و گسترش این خدمات خلاء شبکه ای متمرکز برای نظام‌های پرداخت به وجود آمد. در واقع هنگامی که سرویسی برای گسترش و توسعه محیط کسب و کار ارائه می‌شود وجود مجموعه ای متعهد با چارچوب و قوانین مستند لازم و ضروری است تا سوء استفاده‌ها به حداقل ممکن برسد و همگام با رشد تکنولوژی این سیستم نیز بروز رسانی شود.

روشن است که با پیشرفت و توسعه تکنولوژی با ترکیب ICT می‌تواند خدمات جدیدی را ایجاد کند بنابراین لازم است متناسب با این پیشرفت‌ها چارچوب‌هایی برای حفظ امنیت ایجاد شود زیرا اطلاعاتی که در شبکه انتقال داده می‌شوند اطلاعات شخصی و حریم خصوصی افراد است بنابراین به عنوان مرجع انتقال دهنده اطلاعات باید هم حریم خصوصی رعایت شود و همچنین تکنولوژی باید دارای قواعدی در مسیر داد و ستد باشد.

در واقع رعایت مقررات در جریان سرعت توسعه قربانی شد و از الزامات و مقررات چشم پوشی شد در حالی که قوانین مورد نیاز توسط بانک مرکزی تدوین شده بود اما در جریان رقابت‌های بین موسسات در ارائه خدمات نوین اصل کسب و کار زیر سوال رفت و از منابع عمومی برای هزینه این پیشرفت‌ها هزینه شد.

وقتی کنترل نباشد الزام بر رعایت مقررات و پاسخ گویی نیز نخواهد بود در این خصوص لازم بود تا هرینه فایده‌ها در محیط کسب و کار بررسی شود بنابراین با توجه به دامنه وسیع مبادلات مالی که از یک شعبه عبور می‌کنند لزوم انضباط و اجرای مقررات و اطمینان از اجرای آنها خلاء ساز و کار و یکپارچه بیشتر نمایان شد بنابراین با توجه به سطح معاملات روزانه در سیستم بانکی مطالعاتی در این زمینه صورت گرفت و نتیجه این بود که تقریبا هیچ کشوری نیست که برای نظام پرداخت خود از یک ساز و کار یکپارچه استفاده نکند.

با بروز امکان انجام خدمات بانکی دور از شعبه و خارج از بانک باید فعالیت‌های آنها به صورت یکپارچه و متمرکز توسط موسسه ای که مولود بانک شبکه بانکی است مدیریت شود.

آیا لزوم وجود چنین موسسه ای پس از بروز مشکلات امنیتی در سیستم بانکی به وجود آمد؟

قطبی: خیر حجم بزرگ مبادلات و گردش مالی بود که نیاز به انضباط دقیق تر را قبل از مسائل مالی ایجاد کرد زیرا با وجودانجام تراکنش‌های بانکی دور از شعبه و انتقال پول از حسابی به حساب دیگر، مقررات الزاما اجرا نمی‌شد. در واقع مسئولیت دستگاه‌های pos تسهیل داد و ستد است در حالی که پس از مدتی این دستگاه‌ها به شعبه تبدیل شدند این اتفاق الزامی برای وجود سیستمی همچون شاپرک را ایجاد کرد زیرا خدمات بانکی نیاز به تعریف، اجرای این تعریفات و نظارت بر اجرای آنها بود و نبود چنین سیستمی ممکن بود منجر به بروز فاجعه در شبکه بانکی شود.

در واقع احتمال نشت اطلاعات در شبکه بانکی و خدمات مبتنی بر IT در محیط مجازی وجود دارد، بنابراین لازم است تا قبل از وقوع تا جایی که امکانات و تکنولوژی اجازه می‌دهد مانع از نشت اطلاعات شویم یعنی به روشی عمل کنیم که نشت اطلاعات به خودی خود امکان پذیر نباشد. نکته مهم تر این است که پنلی وجود داشته باشد که در صورت نشت اطلاعات و نفوذ به آنها بتوانیم آن رویداد را مدیریت کنیم. تلاش بر این است که روش‌ها به صورت مداوم بازنگری و توسعه داده شوند تا شرایط ارائه خدمات قابل اطمینان همیشه امکان پذیر باشد. و در صورت بروز یک رویداد امنیتی مقابله سریع با بحران مدیریت شود.

جهت اطمینان از رعایت مقررات از سوی شرکت‌های PSP چه اقداماتی صورت می‌گیرد؟

قطبی: در این خصوص مدیر کارگروه امنیت شرکت‌های PSP جلسه‌های هفتگی با این شرکت‌ها برگزار می‌کند تا رویدادهای که بیانگر ضعف‌های سیستم هستند که موجب رخداد امنیتی می‌شود را بررسی و تبادل نمایند و راه‌های پیشگیری را مشخص کنند. یکی از مزایای یکپارچه سازی و نظارت بر سیستم تشکیل فوری این کمیته در مواقع اضطرار است.

علاوه بر آن رعایت دقیق اصول و چارچوب‌های تدوین شده از سوی شرکت‌های PSP به صورت مداوم پایش و ممیزی می‌شود و عملکرد آنها نظارت می‌شود این نظارت علاوه بر تراکنش در خصوص کسب و کار آنها نیز صورت می‌گیرد تا برای کسب سود بیشتر اقدام به دورزدن مقررات نکنند. همچنین نظارت بر اجرای دقیق مقررات ابلاغی از سوی بانک مرکزی کنترل می‌شود تا همه ذینفعان این مقررات را به درستی انجام دهند. همچنین در کنار آن برای توسعه کسب و کار و ایجاد خلاقیت‌هایی در این زمینه فعالیت می‌کنیم و درکنار این فعالیت‌ها نظارت PSPها را نیز انتقال می‌دهیم اگر

در موردی آئین نامه ای وجود ندارد اقدام به تدوین آن نماییم تا در صورت تایید بانک مرکزی اجرایی شود.
راه اندازی سیستم‌ها تا حدودی توسعه پیدا کرده است و اکنون نیز در حال الویت بندی مجموعه وظایف و تکالیفی هستیم که بر عهده ما گذاشته شده است مثلا توسعه کسب و کار یکی از وظایفی است که در الوین نخست نیست البته این امر در آینده بیشتر مورد توجه قرار خواهد گرفت تلاش ما در حال حاضر بر این است در حالی که کارت بانکی وجود دارد دیگر نیازی به پول نقد نباشد بنابراین در نظارت بر PSPها باید کیفیت تراکنش‌ها نیز کنترل شود که به تمام تراکنش‌ها پاسخ دهند.

چه زیر ساخت‌هایی جهت راه اندازی شاپرک فراهم شد؟

قطبی: در مقطع راه اندازی شاپرک به جای اینکه تمام امکانات و سرویس همانند سوئیچ و دیتا سنتر از اول ایجاد شوند از امکانات موجود در کشور استفاده شد همچنین در مورد منابع انسانی نیز محدودیت‌هایی وجود داشت زیرا افرادی که تجربه پیاده سازی، راه اندازی و مدیریت شبکه را داشته باشند زیاد نیستند بنابراین با توجه به اینکه قرار بود از شبکه ملی پرداخت استفاده شود از منابع موجود در کشور استفاده شد. بنابراین در زمانی کوتاه برای جلوگیری از آسیب دیدن کسب و کار و توسعه خدمات قسمت عملیات و سوئیچ به شرکت خدمات انفورماتیک سپرده شد تا دیتا سنتری که این تراکنش‌ها را انجام می‌دهد بتواند تمام الزامات مورد نیاز را فراهم کند.

در جهت حفظ امنیت در خود سیستم شاپرک و PSPها چه اقداماتی صورت گرفته است و چه الزاماتی باید فراهم شود ؟

قطبی: الزامات مورد نیاز شامل الزامات فنی و الزامات امنیتی می‌شوند. الزامات فنی فعالیت‌هایی هستند که از زمان استفاده از کارت در دستگاه‌ها تا رسیدن اطلاعات به شاپرک صورت می‌گیرند. ممیزی و پایش این فعالیت‌ها و نظارت بر عملکرد PSPها و رویدادهای امنیتی در شبکه انتقال نیز جزء اقدامات امنیتی شاپرک است. همچنین ایجاد چارچوب امنیتی معین در خدمات مبتنی بر بانکداری الکترونیک در شبکه بانکی از جمله فعالیت‌هایی است که توسط شاپرک انجام شده است.
در تدوین این چارچوب از PSADSS.....، مقررات بالادستی ابلاغی رگولاتور، نظرات PSPها و اسناد بالادستی و تجربیات دیگران در موارد مشابه استفاده شده و چارچوبی متناسب با شرایط بومی کشور تدوین شده است.
فعالیت‌های شاپرک مدت زمانی پیش از اعلام رسمی آغاز به کار آن شروع شده بود و در واقع مطالعات در زمینه تدوین چارچوب امنیتی در حال انجام بود در این زمینه تلاش بر این بود که از PSPها نیز دخیل شوند بنابراین کارگروه امنیت تشکیل شد نظرات جمع آوری شد و پس از بررسی و مطالعه به اطلاع اعضاء رسید. در واقع در تدوین این سند از تجربه بازار پرداخت کشور استفاده شد. پس از تایید این سند توسط بانک مرکزی زمانبندی مشخصی در اختیار PSPها قرار گرفت تا الزامات لازم را فراهم نمایند. پیاده سازی این الزامات در سه فاز صورت گرفت و در پایان هر دوره نظارت بر اجرای صحیح انجام شد.
البته این مسئله فقط در مورد مسائل امنیتی نبود بلکه در بعد کیفیت نیز مورد توجه بود مثلا در ارتقاء امنیت از استانداردهای موجود دنیا استفاده از جمله ISO ۲۷۰۰۰ هزار استفاده شد و برآوردی انجام شد تا هزینه ی صورت گرفته در مورد امنیت متناسب با ریسک موجود باشد و لایه‌های امنیتی در سطوح مورد نیاز تامین شوند یعنی اگر موضوع در سطح امنیت ملی است و لایه‌های امنیتی چهارم مورد نیاز است سطح مورد نیاز تامین شود و نه بیشتر یا کمتر از آن.
در حال حاضر ما در آغاز کار هستیم و حدود دو سه سال زمان نیاز داریم تا مجموعه کامل تری داشته باشیم امروز میزان هزینه در حدی است که ممکن است در آینده نیاز به تغییر داشته باشد.

با توجه به الزاماتی که تدوین شده آیا بخشی از این سند قابل انتشار هست یا خیر؟

آزادی: البته این سند محرمانه نیست اما بخش‌های زیادی از این سند صرفا برای بازار پرداخت تدوین شده و به صورت رایگان در اختیار PSPها قرار گرفته است اما ممکن است بخش‌هایی از آن در حوزه‌های دیگر شبکه بانکی قابل استفاده باشد.

در خصوص ارتقاء امنیت چه فعالیت‌هایی صورت گرفته است و SOC در کدام مرحله از فازهای انجام شده مورد توجه قرار گرفت؟

آزادی: در روش گام به گامی که انتخاب حالا طبقه ای مورد توجه بود یعنی در گام اول زیر ساخت‌ها فراهم شد یعنی ایجاد شبکه و امنیت شبکه تکنولوژیکی و ابزاری بود در گام دوم فرآیندهایی که روی شبکه کار می‌کنند مورد توجه بود و در گام آخر فرآیند مدیریت امنیت به همین دلیل در گام آخر به SOC رسیدیم که در حال حاضر در اواسط فاز انتهایی هستیم و شرکت‌ها تا حدودی SOC را عملیاتی کرده اند در انتها PSPها باید بتوانند گواهی ISO۲۷۰۰۰ را دریافت کنند.

آیا در خصوص گواهی ISO۲۷۰۰۰ ممیزی‌های داخلی نیز مورد قبول است یا حتما باید گواهی از CBهای اصلی دریافت شود؟

آزادی: خیر دریافت گواهی مورد نظر از شاپرک نیز به منزله کسب استانداردهای لازم خواهد بود و این گواهی کافی است زیرا برای دریافت این گواهی از CBهای اصلی که خارج از کشور هستند باید اسناد امنیتی در اختیار کشورهای دیگر قرار بگیرد که این خود در تضاد با اصول امنیتی است بنابراین دارا بودن سطح امنیت مشخص و تایید آن کافی است. نکته مهم دریافت گواهی داخلی و رسیدن به الزامات مورد نیاز است.

به نظر شما چه چشم اندازی امنیتی را برای آینده در پیش رو داریم؟

قطبی: همه الزامات مورد نیاز تا کنون فراهم شده اند در سال آینده اسناد مورد بازبینی قرار خواهند گرفت و از تجربیات ممیزی‌ها برای تدوین استانداردهای بروز حرکت خواهیم کرد. در واقع در حال حاضر حداقل‌ها تامین شده است و سال آینده به سمت بهتر شدن گام برمی داریم و در تلاش هستیم تا با سرعت تکنولوژی و تغییرات آن هماهنگ شویم و شرکت‌ها را نیز با این تغییرات هماهنگ کنیم تا بتوانیم به سطح قابل قبولی از امنیت برسیم.

بزرگ‌ترین چالش امنیت اطلاعات آگاهی است

با وجود بحث‌هایی که از گوشه و کنار در خصوص کاهش و رفع تحریم‌های فناوری اطلاعات شنیده می‌شود، هنوز شواهد این امر به وضوح مشخص نشده است. البته گذشته از تاثیرات مهمی که رفع تحریم در فضای سیاسی و اقتصادی کشور خواهد داشت. نمی‌توان تحریم‌ها را تنها عامل بازدارنده در مسیر توسعه فناوری اطلاعات دانست. با شهرام آذرور، مدیر فروش منطقه غرب آسیا در هولدینگ ای ام تی در این خصوص به گفتگو نشستیم که شرح آن را در ادامه می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است ؟

مهمترین رویداد تعداد حملات سایبری‌ست که در سال گذشته به کشور عزیزمان صورت گرفته. امروزه جنگ سایبری در صدر شیوه‌های تجاوز به کشورهای جهان قرارداد و متاسفانه کشور ایران نیز صدمات زیادی از این لحاظ دیده که امیدوارم با استفاده از نیروهای متخصص، دانش روز، تلاش مداوم و سیاستگذاری‌های صحیح در سال جاری شاهد کمتر شدن این اتفاقات باشیم.

با توجه به باز شدن فضای اقتصادی و کاهش تحریم‌ها پیش بینی می کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور برای فروش محصولات و تکنولوژی‌های امنیتی داشته باشند ؟

کاهش تحریم‌ها به نوبه‌ی خود سبب بازشدن فضای اقتصادی کشور مان می‌شود امابه تنهایی نمی‌تواند شرکت‌های معتبر را وادار به ورود به بازار ایران نماید. این امرتنها باعث می‌گردد که کمی مشتاق تر شوند. آنچه که باید انجام گیرد معرفی صحیح بازار کشور به آن شرکتهاست. اینکه چه میزان پتانسیل موجود هست. چه میزان امنیت در سرمایه گذاری وجود دارد و بسیاری مسایل زیر ساختی دیگر... آشنایی و اشتیاق بازار ما به استفاده ازتکنولوژی روزدنیا نیز به این امر کمک میکند.

برای نمونه امروزه دنیا به سمت رایانش ابری (Cloud Computing) می‌رود و سرعت ما با این پیشرفت هماهنگ نیست. خب این مسئله در آینده مشکل ساز می‌شود. نه تنها به دلیل دور بودن ازتکنولوژی روز، که افزون بر آن؛ به واسطه‌ی وجود نداشتن زیرساخت لازم بسیاری از شرکت‌های معتبر تمایلی به حضور در ایران نخواهند داشت. ختم کلام اینست که رفع تحریم‌ها به خودی خود کافی نیست. امیدوارم بخش خصوصی و دولتی در کنار هم بتوانند کمک نمایند تا زیرساخت‌ها بیشتر و سریعتر فراهم شوند و پیشرفت ایران عزیزمان نیز در این صنعت شتاب بیشتری بگیرد.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود ؟

به هیچوجه. همواره در عرصه رقابت شاهد حضور محصولات با کیفیت تری بوده ایم. مهندسین و متخصصین ما در حال حاضر از دانش بالایی برخوردارند اما برای رقابتی سخت تر به دانش خود میافزایند. این امر سبب تقویت و استحکام زیرساخت‌ها خواهد شد و در نهایت موفقیت و رشد روز افزون به ارمغان خواهد آورد.

در همین رابطه آیا ورود شرکت‌های خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

باور دارم که این‌گونه خواهد شد. حضور محصول خارجی در بازار به دلایل بسیاری خوب است اما حضور خود شرکت‌ها و تاسیس شعبه از آن بهتر؛ با این کار میزان سرمایه گذاری افزایش خواهد یافت و نیروهای متخصص ایرانی در شرکت‌های معتبر استخدام می‌شوند. کشوری به وسعت ایران با این منابع غنی و جمعیتی که به تنهایی از جمعیت چند کشور اروپایی بیشتر است؛ به طور حتم برای هر شرکتی وسوسه سرمایه‌گذاری، انتقال تکنولوژی و در مرحله نهایی تولید در ایران برای صادرات به منطقه را به همراه خواهد داشت.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

به هیچ وجه. نه منطقی است و نه می‌توانیم. کشورهایی که در این صنعت پیشرو هستند هم تاکنون نتوانسته اند به این غیرممکن دست یابند. و اصلا نیازی هم به این کار نیست. برای نمونه یکی از بهترین یو تی امهای مطرح دنیا که امریکایی‌ست از آنتی ویروس روسی و پویش محتوای انگلیسی استفاده می کند؛ در حالی که محصولات مشابه امریکایی را در دسترس دارد. پس میبینیم صرف تولید صفر تا صد محصولات نه توصیه می‌شود و نه بهترین کارآیی را دارد. داریم از برداشته شدن تحریم‌ها سخن می‌گوییم. این یعنی به بهترین نرم افزارها و سخت افزارها دسترسی داشته باشیم.

فکر می کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

من همواره بزرگ‌ترین چالش را در مدیریت مدیران ارشد، چه دولتی و چه غیر دولتی دیده ام. البته روی سخنم با همه‌ی عزیزان نیست که بسیاری را می‌شناسم و بسیاری دیگر هم هستند که من نمی‌شناسم اما با اهمیت آی تی و به صورت ویژه امنیت اطلاعات آشنایی دارند؛ اما آن دسته‌ای که به اهمیت این امر آگاه نیستند بزرگ‌ترین چالش را فراهم می‌نمایند. آگاهی نداشتن یعنی باور نداشتن و در نتیجه تحقیقات، توسعه، تولید و حتی خرید در این بخش حمایت نمی‌شود.

به سختی امری بدون حمایت مدیران ارشد و مسئولین امر به موفقیت رسیده باشد. امیدوارم روزی اهمیت این امر برای همگان روشن و واضح باشد تا به جای صرف انرژی برای جلب حمایت به مسایل مهم‌تر و کلان‌تر بپردازیم.

ابـــزار پیشـــرفـــت، تعامل با جهان است

در جهان امروز دیگر نمی‌توان از جهانی شدن اجتناب کرد. حفاظت از اطلاعات در این رویه از اهمیت به سزایی برخوردار است . این جهانی شدن، جهانی سازی و جهانی فکر کردن باید در حالتی صورت گیرد که تهدیدی متوجه امنیت اطلاعات نگردد. گروهی بومی سازی محصولات امنیتی را راهکار این امر می‌دانند و گروهی معتقدند به جهت تحول مفهوم تولید در جهان امروز راهی جز ارتباط با دیگران نیست. آنی خاچکیان مدیر عامل پویه گام که ارائه کننده راه حل‌های جامع شبکه، امنیت در زیرساخت، سیستم مدیریت امنیت، سیستم مدیریت سرویس، سامانه مدیریت امنیت، مدیریت رخداد و مراکز داده است نقطه نظرات خود را در باب امنیت فناوری اطلاعات در سالی که گذشت و آینده آن با ما در میان گذاشته است که در ادامه این گفت‌وگو را می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

مهمترین رویداد افتا در سال ۹۲ به نظر من خبرهای مربوط به اسنودن بود. که بیشتر افکار را متوجه روال‌های حفاظت و آگاهی رسانی به نیروی انسانی کرد. سازمان‌های یادگیرنده که قابلیت ایجاد سیستم‌های به تدریج امن شونده را دارند دارای سه بعد افراد-تکنولوژی-روال‌ها هستند. زمانی سازمان یادگیرنده ایجاد می‌شود که روی هر سه بعد کار هم سو صورت پذیرد در غیر این صورت این مقصود حاصل نمی‌شود. از هر کدام از این بعدها غفلت شود آسیب پذیری در آنجا اتفاق خواهد افتاد.

با توجه به باز شدن فضای اقتصادی کاهش تحریم‌ها پیش بینی می‌کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور را جهت فروش محصولات و تکنولوژی‌های امنیتی داشته باشند؟

تجهیزات امنیتی از آخرین تجهیزاتی هستند که تحریم از روی آنها برداشته خواهد شد. لذا فکر نمی‌کنم تا یک سال آینده شرکت‌های خارجی تحرک بزرگی در ایران انجام دهند.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟

رقابت، جهانی سازی، جهانی تولید کردن،جهانی فکر کردن زمانی تبدیل به تهدید می‌شود که بخواهیم در چارچوب‌های محدود محلی خود را محصور و محدود کنیم و اجازه خلاقیت و انعطاف پذیری را به خود ندهیم. در جهان امروز دیگر نمی‌توان از جهانی شدن اجتناب کرد و اجتناب از آن بیشتر از هر چیز به خودمان ضربه خواهد زد. این مطلب کاملا به سطح جهان بینی و روش ایجاد مزیت‌های تجاری خود تولید کننده بستگی پیدا می‌کند. اینکه تولید کننده مزیت رقابتی اش را چگونه تعریف می‌کند.

در همین رابطه آیا ورود شرکت‌های خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

البته، تماس با بازارهای جهانی تماس با نقطه نظرهای جهانی، ساختارهای جهانی، دغدغه‌های کسب وکار در ابعاد جهانی باعث بالا رفتن بلوغ، دانش و تکنولوژی شرکت‌های داخلی می‌شود.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

پرسش شما مانند این است که بپرسید آیا ایران خودرو لازم است همه قطعات را در ایران تولید کند؟ در جهان امروز دیگر مفهوم تولید، الزام و...تغییر کرده است. این موضوع یک موضوع چند بعدی است که یک بعد آن اقتصاد است که بعد مهمی است و من متخصص آن نیستم لذا من از لحاظ تخصص خود تنها می‌توانم بگویم لازم است با جهان تعامل داشت. لازم است در تولیدات داخلی جهانی فکر کرد. و دانش را در سطح جهانی در دانشگاه‌ها و مراکز علمی پرورش و آموزش داد.

فکر می‌کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

به عقیده ی من بزرگ ترین چالش استاندارد سازی روال‌های امنیتی برای سازمان‌ها، بالا بردن سطح آگاهی در زمینه‌ی تکنولوژی‌های زیرساختی و امنیتی بکار رفته در سازمان است.

لطفا ضمن معرفی کامل خود خلاصه ای فعالیت‌های شرکت را بیان فرمایید

من آنی خاچکیان، مدیرعامل شرکت پیشگامان وادی شبکه‌های یکپارچه (پویه گام) هستم. شرکت ما ارائه کننده راه حل‌های جامع شبکه، امنیت در زیرساخت، سیستم مدیریت امنیت، سیستم مدیریت سرویس، سامانه مدیریت امنیت و مدیریت رخداد و مراکز داده است. ما مفتخریم که با شعار همواره همراه شما هستیم خدمات خود را در سطحی ارائه می‌دهیم که سفارشی سازی شده با نیاز کارفرما باشد تا در این ارتباط برنده-برنده-برنده که برقرار می‌شود نه تنها شرکت ما، شرکت کارفرما بلکه نسل آینده نیز برنده باشند. به نظرمن نظرات مربوط به سازمان‌های یادگیرنده هستند که سبب می‌شود این نوع ارتباط شکل بگیرد و سازمان‌ها را به سوی بلوغ در فاوا ببرد.

پهنای باند بالا؛ تهدید امنیت اطلاعات

افشاگری‌های ادوارد اسنودن از جاسوسی‌های سازمان امنیت ملی آمریکا یکی از خبرساز ترین رخدادهای سال ۹۲ بود. این اتفاق باعث تنش‌های بزرگ در داخل و خارج آمریکا گردید. آگاهی از جاسوسی آمریکا سبب گردید کاربران حوزه فناوری اطلاعات حساسیت بیشتری برای امنیت اطلاعات خود به خرج دهند. شرکت ایمن رایانه پندار با ۱۵ سال سابقه همکاری با شرکت پاندا نقش به سزایی در ایجاد امنیت در فضای سایبری ایران ایفا می‌کند. در باب رخدادهای امنیت فناوری اطلاعات به گفت و گو با قائم مقام این شرکت رضا پرسته نشستیم که در ادامه می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

یکی از بزرگترین اتفاقاتی که امسال دنیا را تکان داد، افشاگری‌های ادوارد اسنودن از جاسوسی‌های سازمان امنیت ملی امریکا بود. این مهم بازتاب بسیاری در کشورهای گوناگون از جمله ایران داشت. طبعا علم به این موضوع که NSA از چه راه‌های گوناگون و شگفت آوری برای جمع آوری و شنود اطلاعات در سراسر دنیا استفاده می‌کند، موجب خواهد شد تا دولت‌ها و حتی کاربران حساسیت بیشتری برای امنیت اطلاعات خود به خرج دهند. در ایران نیز امسال این ذهنیت که باید تا جایی که امکان دارد، بستر فناوری اطلاعات و ارتباطات بومی شده و گردش اطلاعات مهم را در حیطه مرزهای خود نگه داشت، در بین مدیران دولتی بسیار پر رنگتر از گذشته شده است. این دیدگاه البته به فناوری ابر و گسترش بازار پردازش ابری Cloud Computing لطمه شدیدی زده است. اما ما باید مجازی سازی و پردازش ابری را که آینده ناگزیر فناوری اطلاعات است، بپذیریم و در جستجوی راهکارهای امنیت اطلاعات در فناوری ابر باشیم.

با توجه به بازشدن فضای اقتصادی و کاهش تحریم‌ها پیش بینی می‌کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور برای فروش محصولات و تکنولوژی‌های امنیتی داشته باشند؟

بازار مصرفی ایران برای شرکت‌های خارجی با توجه به رقم‌های مبادله شده در این بازار وسوسه کننده است. چراکه حتی در شرایط تحریم نیز محصولات خارجی در ایران حضور پررنگی داشته اند. هرچند شرکت‌های خارجی مجبور بوده اند تا رابطه با ایران را انکار کنند. با برچیده شدن تحریم‌های بین المللی چند اتفاق مثبت در این بازار خواهد افتاد. مهمترین اتفاق حضور رسمی این شرکت‌ها و بسیاری شرکت‌های دیگر در ایران است. این رخداد در عین حال که سبب افزایش تنوع محصولات و ایجاد رقابت سازنده خواهد شد، از دیگر سو به افزایش کیفیت خدمات پس از فروش نیز کمک شایانی خواهد کرد. امروزه یکی از بزرگترین دغدغه‌های مصرف کنندگان محصولات خارجی، نحوه ضعیف دریافت خدمات پس از فروش است. اتفاق دیگر این است که قیمت‌های محصولات کاهش خواهد یافت و موجب اقبال بیشتر مصرف کنندگان سازمانی و خانگی به استفاده از تکنولوژی روز دنیای IT خواهد گردید.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟ در همین رابطه ورود شرکت‌های خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

اگر نگاه بلند مدت به این مسئله داشته باشیم، برای محصولات بومی تهدیدی به وجود نخواهد آمد. ورود تکنولوژی روز دنیا به تولید کنندگان بومی اجازه خواهد داد تا با تعامل سازنده با تولیدکنندگان خارجی در دراز مدت در جهت افزایش سطح کیفی و کمی محصولات خود همت گمارند. و حتی بتوانند مانند تولیدکنندگانی که در چین، هند، تایوان و... به دنیا سرویس می‌دهند، پا را از مرزها فراتر گذاشته و جهانی شوند.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

دو دیدگاه وجود دارد. دیدگاه فنی و دیدگاه امنیتی. از جنبه فنی هر شرکتی برای ارائه بهینه یک محصول، به همکاری با سایر شرکت‌ها (Joint Vendor) فکر می‌کند. بهترین برندها و محصولات را در کنار هم جمع کرده و در نهایت یک محصول جامع و در عین حال با کیفیت ارائه می‌کند.

اما از جنبه امنیتی و به خصوص پس از افشاگری‌های اسنودن، همیشه بیم آن می‌رود که استفاده از تکنولوژی‌ها و محصولات خارجی تیشه به ریشه امنیت ملی بزند. اما اگر بخواهیم صادق باشیم، ما تا تولید بسیاری از محصولات، به ویژه سخت افزارهای گوناگون در ایران راه درازی در پیش داریم. پس بهتر است به جای رها کردن تکنولوژی‌های روز دنیا به بهانه‌های امنیتی، همزمان با بومی سازی، برای افزایش نسبی امنیت اطلاعات از محصولات مناسب خارجی نیز استفاده نماییم.

فکر می‌کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

همانگونه که پیشتر اشاره شد، یکی از چالش‌ها می‌تواند کنار آمدن بخش دولتی و عمومی با امنیت فناوری ابرCloud Security باشد. چراکه هر روز ما شاهد گسترش این فناوری در سطح زیر ساخت Iaas و به ویژه نرم افزار Saas هستیم. اگر قرار باشد برخورد ما با فناوری ابر شبیه برخورد دهه ۷۰ ما با اینترنت باشد، طبعا با سرعت بیشتری از تکنولوژی روز جا خواهیم ماند.

از دیگر تهدیدهای توسعه امنیت فناوری اطلاعات کمبود بودجه است که سال‌هاست پابرجاست. ارائه پهنای باند بالا که در دستور کار دولت است، نیز از دیگر تهدیدهای امنیت بشمار می‌رود. هرچه سرعت وبگردی و سهولت دسترسی به اینترنت افزایش یابد، اینترنت جای خود را بیشتر در زندگی روزمره آدمی باز می‌کند و به مثابه آن حملات سایبری و آلودگی بدافزارها نیز افزایش خواهد داشت. شاهد این ادعا نیز حمله‌های هکرها به ماشین‌های هوشمند خانگی نظیر یخچال‌ها، مایکروفرها و ... است.

تولید محصولات امنیتی بومی با استفاده از دانش موجود امکان‌پذیر است

افشاگری‌های اسنودن از سوی بسیاری از کارشناسان امنیتی جهان مسئله مهمی در حوزه امنیت فناوری اطلاعت بود که موجب حساسیت یافتن مسئله امنیت اطلاعات در فضای سایبر شد. حفظ امنیت اطلاعات چه در سطح ملی و بین المللی و چه در سطح فردی موضوعی بسیار حائز اهمیت است که نادیده گرفتن آن می‌تواند خسارات جبران ناپذیری وارد کند. حمیدرضا مختاریان مدیر ارشد ارشد فناوری و امنیت شرکت توسن در گفت و گویی دیدگاه‌های خود در خصوص امنیت اطلاعات را به ما اشتراک گذاشت که شرح آن را در ادامه می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

به نظر من ماجرای ادوارد اسنودن یکی از مهمترین رویدادهای اخیر در زمینه افشاگری اطلاعات محرمانه بوده است. اگرچه این ماجرا بیشتر ماهیت جاسوسی دارد، اما از دو دیدگاه در این حوزه حائز اهمیت است.از دیدگاه اول، این مساله موجب گسترش جو بی اعتمادی، افزایش بدبینی و ایجاد فضای نا امن جهت تولید و تبادل اطلاعات و ارتباطات شده است. تا جاییکه، امنیت اطلاعات را با چالشی جدی روبرو کرده است وتبعات منفی ناشی از آن در آینده نیز همچنان ادامه خواهد داشت. از سوی دیگر، می‌توان جنبه مثبت افشاگری اطلاعات توسط اسنودن و افزایش توجه به این حوزه را نیز مورد توجه قرار داد.

با توجه به باز شدن فضای اقتصادی و کاهش تحریم‌ها، پیش بینی می‌کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور، جهت فروش محصولات و تکنولوژی¬های امنیتی داشته باشد؟

بدیهی است که تمایل ورود شرکت‌های خارجی به بازار کشور با کاهش تحریم‌ها و باز شدن فضای اقتصادی بسیار زیاد خواهد بود، بنابراین محصولات و تکنولوژی‌های امنیتی نیز از این قاعده مستثنی نیست.

آیا این مساله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟

با توجه به اینکه امروزه بسیاری از حملات و همچنین روش‌های مقابله با آنها به سمت لایه کاربرد (application) رفته است و از آنجا که توانایی استفاده از ابزارهای حفاظتی در این لایه برای تولید کنندگان بومی به مراتب بیشتر است، لذا این مساله نمی‌تواند تهدیدی به شمار آید. از طرف دیگر هر کشوری می¬تواند با دانش بومی خود محصولاتی با کارایی موثرتر تولید کند.

در همین رابطه آیا ورود شرکتهای خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

بله حتما. با استفاده از تکنولوژی‌های جهانی می‌توان از طیف گسترده تری از دانش و ابزار برای تولید محصولات بومی قوی بهره برد.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

خیر، چرا که همواره تعاملات با کشورهای توسعه یافته و استفاده از تجربیات، دستاوردها و نتایج علمی آنها منجر به تولید محصولات پرثمر و متنوعی خواهد شد.

فکر می‌کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

به نظر من کمبود نیروی انسانی متخصص یکی از مهمترین چالش‌های پیش رو در این زمینه خواهد بود. به علاوه، کمبود ابزار کافی و دانش به روز موجب کاستی‌هایی در این زمینه شده است. همچنین می‌توان به چالش‌های موجود در زمینه رایانش ابری و شبکه‌های اجتماعی و مسایل امنیتی مرتبط با آنها اشاره کرد. از سوی دیگر، مسایل چالش بر انگیزی مانند زیست سنجی (Biometric) و احراز هویت (Authentication) باید مورد توجه قرارگیرند. بنابراین باید در سطح کلان به بررسی این چالش‌ها پرداخت و پیش بینی‌ها و تدابیر لازم را به کارگرفت.

در پایان ،ضمن معرفی کامل خود، خلاصه ای از فعالیت‌های شرکت را بیان فرمایید.

حمید رضا مختاریان، مدیر ارشد فناوری و امنیت شرکت توسعه سامانه‌های نرم افزاری نگین (توسن).

چنانچه دیدگاه خاصی در مورد فناوری‌های جدید و ارتباط آن با امنیت از جمله فناوری رایانش ابری، تجهیزات پوشیدنی و ... دارید، بیان نمایید.

یکی از بزرگترین چالش‌های حوزه بانکداری، هزینه‌های بالا در ایجاد زیر ساخت لازم جهت پیاده سازی تکنولوژی‌های پیشرفته و عدم استفاده بهینه از تجهیزات می‌باشد. رایانش ابری استفاده از سرویس‌های اشتراکی بر روی بستر اینترنت را فراهم می‌آورد و نقش بزرگی را در حل مشکل مذکور، بدون نیاز به هزینه‌های اضافی، ایفا می‌کند. اخیراً رایانش ابری در حوزه بانکداری مورد پذیرش قرار گرفته است و بانک‌ها و موسسات مالی با در نظر داشتن شرایط احتیاط در پی حداکثر استفاده از آن می‌باشند. مسائل امنیتی، تطابق با قوانین، محافظت از اطلاعات مشتریان و حفظ حریم شخصی آنها جزو مسائل مهمی می‌باشد که زمینه ساز ایجاد تردید در مدیران شده است.لذا در حوزه‌های حساس از جمله بانکداری، در نظر داشتن موارد امنیتی از سوی سازمان‌های بالادستی و قانون گذار و ارائه ملزومات و دستورالعمل‌ها می‌تواند از سیلی از مشکلات آتی پیشگیری نماید.

سال ۹۳ بدون تغییر برای محصولات امنیتی

سال ۹۲ در مقایسه با سال گذشته شاهد مخاطرات امنیتی کمتری در داخل کشور بود و می‌توان گفت آرامش بیشتری بر بازار امنیت حاکم بود. اما این مسئله باعث نخواهد شد که امنیت فضای سایبر اهمیت خود را از دست بدهد. در هر حال متخصصان امنیتی معتقدند که امنیت مسئله مهمی است که لازم است دانش مرتبط با آن پیوسته بروز شود. در روزهای پایان سال ۹۲ به سراغ اکبر احمدی مدیر عامل شرکت تجارت امن رفتیم تا دیدگاه وی در خصوص امنیت در سال ۹۲ را بشنویم در ادامه شرح این گفتگو را می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

در حوزه امنیت فناوری اطلاعات اتفاق بارز و قابل ذکری روی نداده است اما در حوزه فناوری اطلاعات ابلاغ شرح وظایف دبیرخانه شورای عالی فضای مجازی از نظر من مهمترین رویداد در سال ۹۲ بوده است.

با توجه به بازشدن فضای اقتصادی و کاهش تحریم‌ها پیش بینی می‌کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور را برای فروش محصولات و تکنولوژی‌های امنیتی داشته باشند؟

محصولات امنیتی در دسته‌ی تکنولوژی خاص و بالا قرار می‌گیرند لذا به نظر نمی‌رسد سال آینده شاهد تغییر خاصی در این زمینه باشیم.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟

اصولا ما باید به فکر تولید محصولات بومی باشیم تا حد امکان از Back Door جلوگیری نماییم. اما به نظر نمی‌رسد شرکت‌های خارجی تولید کننده این نوع محصولات در سطح متوسط و پایین تهدیدی برای محصولات داخلی باشند. اما در هر صورت تولید محصولات امنیتی بومی از می‌تواند در ایجاد امنیت پایدار موثر باشد.

در همین رابطه آیا ورود شرکت‌های خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

آن چیزی که مشخص است، محصولات با تکنولوژی بالا امکان مهندسی معکوس را به سختی فراهم می‌کند؛ اما میزان استفاده از ایده‌های آنان مناسب است.

شما لازم می‌دانید که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

بله؛ زیرا رابطه‌ی مستقیم با امنیت ملی داشته و نباید در این زمینه وابستگی وجود داشته باشد.

فکر می‌کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

با گسترش فضای تبادل الکترونیکی مبحث امنیت نیز به صورت جدی باید پیگیری شود به خصوص این‌که ما از لحاظ سیستم‌های جلوگیری از حملات سایبری دارای ضعف هستیم، و باید با راهکارهای مختلف خود را واکیسنه نماییم.

لطفا ضمن معرفی کامل خود، خلاصه‌ای از فعالیت‌های شرکت را بیان فرمایید.

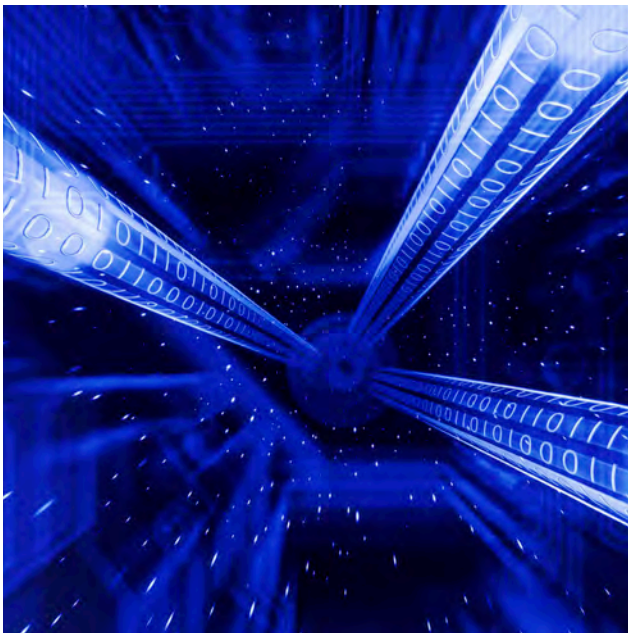
اکبر احمدی مدیر عامل شرکت تجارت امن خاورمیانه

شرکت تجارت امن یکی از شرکت‌های فعال در ارائه کننده راهکارهای امنیت شبکه، سیستم‌های جمع آوری و پردازش اطلاعات است.

در پایان چنانچه دیدگاه‌های خاصی درباره‌ی فناوری‌های جدید و ارتباط آن با امنیت از جمله فناوری رایانش ابری، تجهیزات پوشیدنی و ... دارید، بیان نمایید.

با گسترش استفاده از فناوری شبکه‌های بی سیم و فناوری‌های جدید باید به فکر امن کردن فضای تبادل اطلاعات نیز باشیم. زیرا هر چه امکان دسترسی به فناوری اطلاعات بیشتر شود حفظ امنیت در آن مهمتر خواهد بود و لازم است بیشتر مورد توجه قرار گیرد.

محصول امنیتی بومی نیاز مراکز حساس و حیاتی کشور است



توسعه ابزارهای بومی امنیتی با توجه به خطراتی که در فضای سایبر وجود دارد امری بدیهی است. که تمامی دست اندر کاران حوزه امنیت بر اهمین آن اذعان دارند اما در خصوص چگونگی نگاه به این مسئله و ساز و کارهای تولید محصولات بومی نظریه‌های متفاوتی در بین کارشناسان و متخصصان این امر وجود دارد با علیرضا منافی مدیر عامل شرکت امن افزار گستر شریف به گفتگو نشستیم تا با دیدگاه‌های او در این خصوص بیشتر آشنا شویم. شرح این گفتگو را در ادامه می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

حمایت دولت از تولید در سال حماسه اقتصادی انتخاب دولت جدید حامی سندیکاها و بخش خصوصی و فعال شدن مجدد شورای عالی فضای مجازی مهمترین رویدادهای سال جاری در حوزه ICT بوده است.

با توجه به بازشدن فضای اقتصادی و کاهش تحریم‌ها پیش بینی می‌کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور را جهت فروش محصولات و تکنولوژی‌های امنیتی داشته باشند؟

با توجه به بخشنامه‌های ممنوعیت محصول امنیتی خارجی و نیز حمایت‌های وزارت صنایع از تولید ملی تاثیر بسیار کمی خواهد داشت.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟

به نظر من بیشتر موجب ایجاد بازار رقابتی و بهبود محصولات داخلی خواهد شد. و تولیدکنندگان محصولات بومی برای اینکه بتوانند در این بازار باقی بمانند تلاش بیشتری جهت افزایش کیفیت تولیدات خود خواهند کرد.

در همین رابطه آیا ورود شرکت‌های خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

بله در صورت لزوم ایجاد هم افزایی داخلی و خارجی محتمل است.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

بله تولید محصولات بومی امنیتی با تکنولوژی و دانش کاملا داخلی جهت شناخت ابعاد مختلف امنیت فضای تولید و تبادل اطلاعات و استفاده و بهره برداری در مراکز حساس و حیاتی کشور جهت جلوگیری از تهدیدات احتمالی لازم است.

فکر می‌کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

بیش‌ترین چالش سال آینده در بعد تأمین اعتبار و بودجه افتای سازمان‌ها خواهد بود که با توجه به افزایش روزافزون تهدیدات سایبری، از یک سو سازمان‌ها در معرض انواع آسیب‌پذیری‌های جدی در فناوری اطلاعات و ارتباطات قرار گرفته اند و از سوی دیگر توان مالی شرکت‌های ارائه دهنده خدمات و محصولات افتا به چالش کشیده خواهد شد که خطری بزرگ برای امنیت ملی خواهد بود.

در پایان، لطفا ضمن معرفی کامل خود، خلاصه ای از فعالیت‌های شرکت را بیان فرمایید.

امن‌افزار گستر شریف با بیش از یک دهه سابقه به عنوان یک شرکت رسمی دانش بنیان حوزه افتا با ارائه سبد کاملی از خدمت و محصولات امنیت شبکه و اطلاعات در حوزه‌های مختلف استراتژی‌های امنیت، نظام‌های مدیریت امنیت، ارائه انواع تجهیزات دیواره آتش و UTM، ارائه راهکارهای زیرساخت کلیدعمومی مبتنی بر رمزنگاری نامتقارن، ثبت انواع ادله‌های الکترونیکی، تأمین امنیت پایانه‌های کاری و سرورها و تجهیزات شبکه و استقرار ساختارهای دفاع امنیتی مبتنی بر SOC/ Cert جامع‌ترین راهکارهای یکپارچه امنیتی را به طیف گسترده‌ای از مشتریان خود ارائه می‌دهد.

بازار ایران، بازار قابل رقابت برای شرکت‌های خارجی

از زمانی که امنیت به یکی از دغدغه‌های مهم فعالان حوزه فناوری اطلاعات کشور و البته کاربران آن تبدیل شد همواره تولید محصولات بومی امنیتی نکته ای مهم و مورد بحث بوده است. بسیاری از تولید کنندگان و حتی واردکنندگان محصولات امنیتی معتقدند که اعتماد کامل به محصولات امنیتی غیربومی و سهل انگاری در حوزه امنیت منجر به وارد آمدن صدمات جبران ناپذیر خواهد شد. دیدگاه‌های ایمان فکری مدیر عامل شرکت آیکو یکی از شرکت‌های فعال در حوزه امنیت اطلاعات را در ادامه می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

اقبال فزاینده بازار و به خصوص سازمان‌های دولتی برای تقویت زیر ساخت‌ها در جهت افزایش ضریب امنیت اطلاعات را می‌توان به عنوان یکی از مهمترین رویدادهای این حوزه برشمرد.

با توجه به باز شدن فضای اقتصادی و کاهش تحریم‌ها پیش بینی می کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور برای فروش محصولات و تکنولوژی‌های امنیتی داشته باشند؟

شرکت‌های خارجی تمایل و اشتیاق بسیاری برای ورود به بازار ایران دارند اما با ادعای کاهش تحریم‌ها چندان موافق نیستم چون مابین آنچه در عمل اتفاق افتاده با آنچه از رسانه‌ها منعکس گردیده است، تفاوت زیادی وجود دارد.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟

اگر این موضوع اتفاق بیفتد که به نظر من هنوز اتفاق نیفتاده، بسته به سیاست‌هایی که دولت اتخاذ می کند، دو گزینه پیش رو خواهد بود.

چنانچه این سیاست‌ها مبتنی بر ممنوعیت خرید کالای خارجی (حداقل توسط مشتریان دولتی که بخش بزرگی از بازار را تشکیل می دهند) مبتنی باشد (بدون توجه به اینکه حضور شرکت‌های خارجی تا چه اندازه پررنگ خواهد بود) نه تنها تهدیدی متوجه محصولات بومی نخواهد بود بلکه فرصتی ویژه برای حضور در بازار برای این دسته محصولات ایجاد خواهد شد.

و بالعکس اگر بر اثر کاهش تحریم‌ها، محصولات خارجی امنیتی حضوری پررنگ در بازار پیدا کنند و امکان رقابت برابر باشد بدیهی است در کوتاه مدت چه به لحاظ امکانات و چه به لحاظ قیمت، گوی و میدان در اختیار خارجی‌ها خواهد بود و تنها فرصتی که برای محصولات بومی ایجاد خواهد شد، ضرورت ارتقا کیفی و بهبود قیمتی است که شاید با تعامل جدی و نزدیک با شرکت‌های خارجی ایجاد گردد و در صورت استفاده از این فرصت، امکان رقابت در کلاس جهانی برای این محصولات در آینده فراهم خواهد گردید.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

خیر، این موضوع توسط شرکت‌های صاحب نام بین المللی نیز به صورت صفر تا صد انجام نمی‌شود. برای نمونه تولید کنندگان UTM غالب سخت افزارهای مورد نیاز خود را از شرکت‌های دیگر تهیه می کنند.

فکر می کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

میزان بودجه تعیین شده برای توسعه امنیت اطلاعات و تحریم‌های موجود

در پایان چنانچه دیدگاه‌ها ی خاصی در مورد فناوری‌های جدید و ارتباط آن با امنیت از جمله فناوری رایانش ابری ، تجهیزات پوشیدنی و... دارید، بیان نمایید.

من معتقدم که به زودی تغییراتی بنیادی در تکنولوژی و در حوزه IT اتفاق خواهد افتاد که موج سوم مبتنی بر آن خواهد بود و مهم ترین موضوع آن تکنولوژی Cloud Computing خواهد بود.

بی شک این تکنولوژی که در کشور ما نیز کم و بیش مطرح گردیده و شرکت آیکو نیز با برگزاری سمینارها و کارگاه‌های آموزشی گوناگون، مروج آن بوده است ،تحولات عظیمی در صنعت IT ایجاد خواهد کرد.

برای نمونه همین بس که آقای استیو بالمر، CEO پیشین شرکت مایکروسافت در سال ۲۰۱۱ در سخنرانی خود در دانشگاه واشنگتن اعلام نمود که "هم اکنون بالغ بر ۷۰ درصد از پرسنل شرکت مایکروسافت روی پروژه‌های Cloud computing کار می‌کنند و این رقم در سال ۲۰۱۲ به حدود ۹۰ درصد خواهد رسید."

حضور شرکت‌های خارجی در ایران فرصت؛ نه تهدید

امروزه مقابله با حملات سایبری حجم عظیمی از بودجه کشورها را به خود اختصاص می‌دهد. ضرورت حفاظت از اطلاعات موازی با امنیت کشور محسوب می‌گردد. ایران در سال ۹۲ در مقایسه با سال‌های پیش شاهد کمتر شدن این حملات بود. دلایل این اتفاق نیکو را می‌توان اخلاق مداری بیشتر کشورها در قیاس با گذشته، همچنین پیشرفت فناوری‌های مربوط به این حوزه و افزایش میزان آمادگی کشور دانست. بیت دیفندر جزو معدود شرکت‌های عرضه کننده راهکارهای امنیت نرم افزار با محوریت ضد ویروس در جهان است که حضور مستقیم در بازار ایران دارد. پژمان تجلائی مدیر دفتر بیت دیفندر به پرسش‌های افتانا درباره امنیت فناوری اطلاعات در ایران پاسخ داده است که در ادامه می‌خوانید.

مهمترین رویداد حوزه افتا در سال ۹۲ از دید شما چه بوده است؟

خوشبختانه در سال ۹۲ در مقایسه با سال‌های پیش شاهد حملات سایبری کمتری بودیم. از جمله مهمترین حمله، حمله به سایت‌های وزارت نفت در اواخر خرداد ماه بود. این مهم به دلیل اخلاق مداری بیشتر کشورها در این زمینه در مقایسه با گذشته، و همچنین کسب تجربه و افزایش میزان آمادگی در حوزه‌های مختلف در مواجهه با این موضوع بود. اما به طور کلی می‌توان تاثیر انتخابات ریاست جمهوری و تعیین سیاست‌های جدید و مرتبط در این حوزه با نگاه امیدوارنه به آینده را اشاره داشت که حضور فعال تر شرکت‌ها در نمایشگاه الکامپ امسال نیز گواه آن است.

با توجه به بازشدن فضای اقتصادی و کاهش تحریم‌ها پیش بینی می‌کنید که شرکت‌های خارجی تا چه میزان تمایل به ورود به بازار کشور را جهت فروش محصولات و تکنولوژی‌های امنیتی داشته باشند؟

کشور ایران به دلیل سه مولفه اندازه بازار، جذابیت بازار و رشد بازار که از ویژگی‌های تعیین کننده هر کسب و کار است همواره با توجه شرکت‌های خارجی برای ورود و توسعه فروش روبرو بوده است. بی شک تغییر فضای کسب و کار سبب شتاب دهی بیشتر برای حضور گردیده است. و با توجه به روند حاضر، حرکت به سمت الکترونیکی شدن امور جدای از مزایای بسیار که در ذات این موضوع است یک الزام در فضای جاری است. ایجاد امنیت و استفاده از تکنولوژی‌های امنیتی به عنوان یک باید بر روی بسترهای این جریان خود دلیل دیگری برای جذابیت‌های این حوزه، تمایل بالای شرکت‌های خارجی برای ورود به بازار کشور است.

آیا این مسئله تهدیدی برای تولید محصولات امنیتی بومی خواهد بود؟ورود شرکت‌های خارجی، امکان استفاده از فناوری‌های جدید و انتقال تکنولوژی را برای تولید محصولات بومی فراهم خواهد آورد؟

دنیای امروز در تمامی حوزه‌ها مبتنی دو مفهوم شبکه (Network) و ارتباطات (Communication) بنا شده است. بدین معنا که برای انجام هر فعالیتی ابتدا نیاز به نقاطی برای تعامل و سپس مکانیزم‌هایی برای ارتباط با یکدیگر است. هر چقدر تعداد این نقاط بیشتر و فرآیندهای ارتباطی سریعتر و راحتر انجام گیرد عملکرد بهتری صورت خواهد گرفت. حال با تعمیم همین مفهوم به بازار جهانی، حضور شرکت‌های خارجی نه در جایگاه تهدید بلکه به عنوان فرصت بوده که در تعامل با ایشان می‌تواند عاملی رقابتی برای تشویق تولیدکنندگان داخلی به تلاش و ارائه محصولات بهتر و همچنین استفاده از فناوری‌های جدید و انتقال تکنولوژی بی‌انجامد.

به نظر شما لازم است که از صفر تا صد محصولات امنیتی در داخل کشور تولید شود؟

با توجه به پاسخ پرسش پیشین و همچنین ظرفیت‌ها و توانمندی‌های سخت افزاری و نرم افزاری موجود در کشور این امر می‌تواند در سطوح مختلف امکان پذیر باشد. اما با توجه به مفهوم امنیت در دو حوزه سخت افزار و نرم افزار لازمه این امر مستلزم نگاه درست و کلان محور به این مقوله به همراه سیاست گذاری‌های حمایتی منطقی در این بخش است.

فکر می‌کنید چالش‌های پیش رو در توسعه امنیت اطلاعات (در سطح کلان) در سال آینده چه خواهد بود؟

نبود یک برنامه جامع، درک درست از حوزه امنیت اطلاعات، محدودیت‌های زیر ساختی، کندی ترمیم و توسعه آن به دلیل فقدان منابع، دانش لازم و محدودیت‌های مالی از چالش‌های توسعه امنیت اطلاعات در ایران به شمار می‌رود.

چنانچه دیدگاه‌های خاصی در مورد فناوری‌های جدید و ارتباط آن با امنیت از جمله فناوری رایانش ابری، تجهیزات پوشیدنی و ... دارید، بیان نمایید.

بی شک، مهم ترین فناوری که حوزه IT را در این چند سال و همچنین سالیان آینده تحت تاثیر و تحول قرار داده و خواهد داد فناوری رایانش ابری است. مهم ترین چالش‌های این حوزه عبارت اند از امنیت، استفاده موثر و بهینه، و چالش‌های قانونی و دولتی. هر چند وضعیت فعلی این فناوری در ایران در ابتدایی بوده ولی روند و آینده این فناوری مثبت و صعودی خواهد بود.

از دیگر فناوری‌هایی که در حوزه‌ی امنیت با شیب بالا در حال حرکت است می‌توان به مجازی سازی (Virtualization) اشاره داشت. ضرورت شدید به مدیریت و کاهش انرژی، مدیریت منابع و هزینه‌های سخت افزاری و ایجاد امنیت لازم باعث حرکت آینده با شتاب بالا به این سو خواهد بود. توضیح اینکه بیت دیفندر برای تمامی فناوری‌های اعلامی، راهکارهای منحصر به فردی دارد.

راهنمای تصویری حملات فیشینگ

اخیراً پیش آمده که ایمیل خود را باز کنید و موردی را ببینید که به نظر به فیشینگ شباهت دارد؟ یک پیام از eBay درباره‌ی محصولی که هرگز نمی‌خرید؟ یک یادآور از PayPal برای بروزرسانی حساب، در حالی که اصلا حساب PayPal ندارید؟ یک ایمیل مختصر از بانکی که شش سال پیش در آن حساب داشتید – ولی دیگر مشتری آن بانک نیستید ولی چرا بانک ول‌کن شما نیست؟

شما تنها نیستید. هر هفته میلیون‌ها فیشینگ - نوعی از ایمیل‌های کلاهبردارانه – به مشتریان در سرتاسر جهان ارسال می‌شود.

پیشتر، شناسایی فیشینگ‌ها کاری آسان بود – آن‌ها پر بودند از اشتباهات املایی و تایپی، با ادبیاتی ضعیف که از ایمیل‌ها عجیب‌وغریبی ارسال می‌شدند – ولی آن دوران به سر آمده است. امروزه فیشینگرها از تکنیک‌های به مراتب سطح بالاتری استفاده می‌کنند، و شناسایی هدف کلاهبرداری آن‌ها بسیار دشوارتر شده است.

فیشینگ آنقدر متداول شده است که در سال ۲۰۰۵ دیکشنری آکسفورد کلمه‌ی «phishing» را به آخرین چاپ خود اضافه کرد. این دیکشنری فیشینگ را اینگونه تعریف می‌کند:

فیشینگ /اسم/
عمل کلاهبرداری از طریق ارسال ایمیل‌هایی که ادعا می‌کنند از جانب شرکت‌های معتبر ارسال می‌شوند به منظور اینکه افراد را به افشای اطلاعات شخصی نظیر کلمه‌عبور و شماره کارت‌های اعتباری فریب دهند.

تعداد و میزان پیچیدگی حملات فیشینگ به مشتریان روز به روز در حال گسترش است. در حالی که بانکداری آنلاین و تجارت الکترونیک خیلی ایمن هستند، به عنوان یک قانون کلی، شما باید در مورد افشای اطلاعات شخصی خود بسیار هشیار و محتاط باشید. کار دیگری که می‌توانید انجام دهید این است که در مطلع باشید.

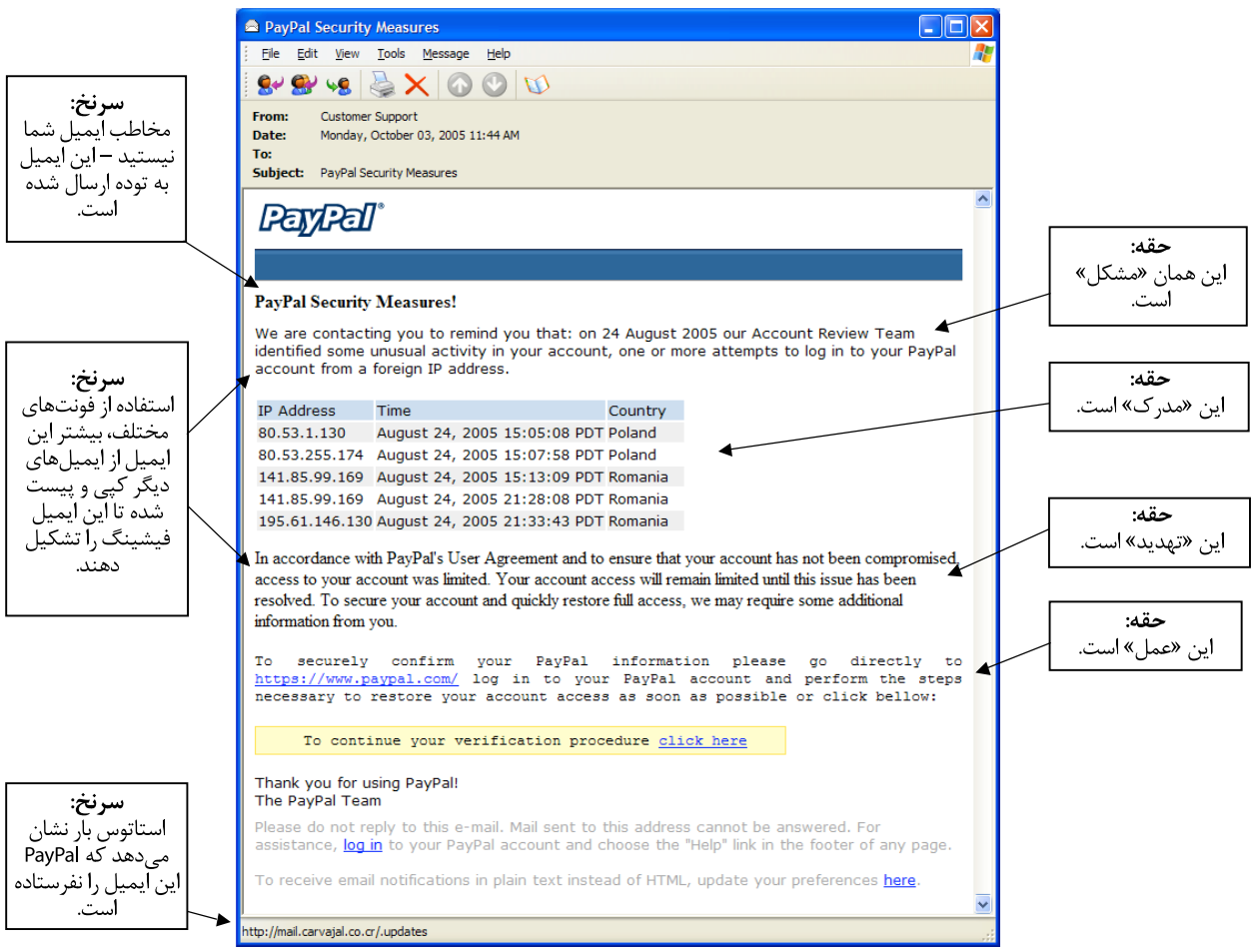
این راهنما، توضیحات مختصر و مفید و نمایش بصری فیشینگ‌های خطرناک و فریبکاری که ممکن است به درون کامپیوترهای شما نفوذ کنند را ارائه می‌دهد. برای کمک به شما در مقابل این تهدیدات، و اعتماد به ایمیل‌های سالمی که به صندوق پستی شما ارسال می‌شوند – در انتهای این راهنما پیشنهادهایی مطرح شده‌اند تا از خودتان مراقبت کنید، همچنین برای اطلاعات بیشتر منابع دیگر حملات فیشینگ معرفی شده‌اند.

ماهی کماندار (Archerphish)

توضیحات: ماهی کماندار یکی از بدذات‌ترین فیشینگ‌ها در دریای ایمیل است. این فیشینگ از یک روش خلاقانه برای حمله به شکار خود استفاده می‌کند – که هم در زیر آب و هم روی آب کاربرد دارد! در واقع، ماهی کماندار برای حملات غیرمعمولش شهرت دارد، مانند شلیک آب با دهانش به طرف قربانی و سقوط آن.

رفتار: این گونه فیشینگ علاقه دارد گیرنده ایمیل را با پیام‌هایی مانند «آن بیرون کسی هست که می‌خواهد به تو آسیب برساند» فریب دهد. ماهی کماندار ممکن است ادعا کند که تلاش‌های ناموفق متعددی به حساب شما صورت گرفته و یا اینکه کسی در حال استفاده از حساب eBay شما است و پیشنهادهای اشتباهی را برای مزایده‌ها ارسال می‌کند. این کلاهبرداری‌ها را باور نکنید!

حقه: مشکل را مطرح می‌کند، مدرک ارائه می‌دهد، شما را تهدید می‌کند اگر کاری نکنید با مشکلات بیشتری مواجه خواهید شد، و سپس یک لینک به شما می‌دهد تا روی آن کلیک کنید و «مشکل» خود را حل کنید.

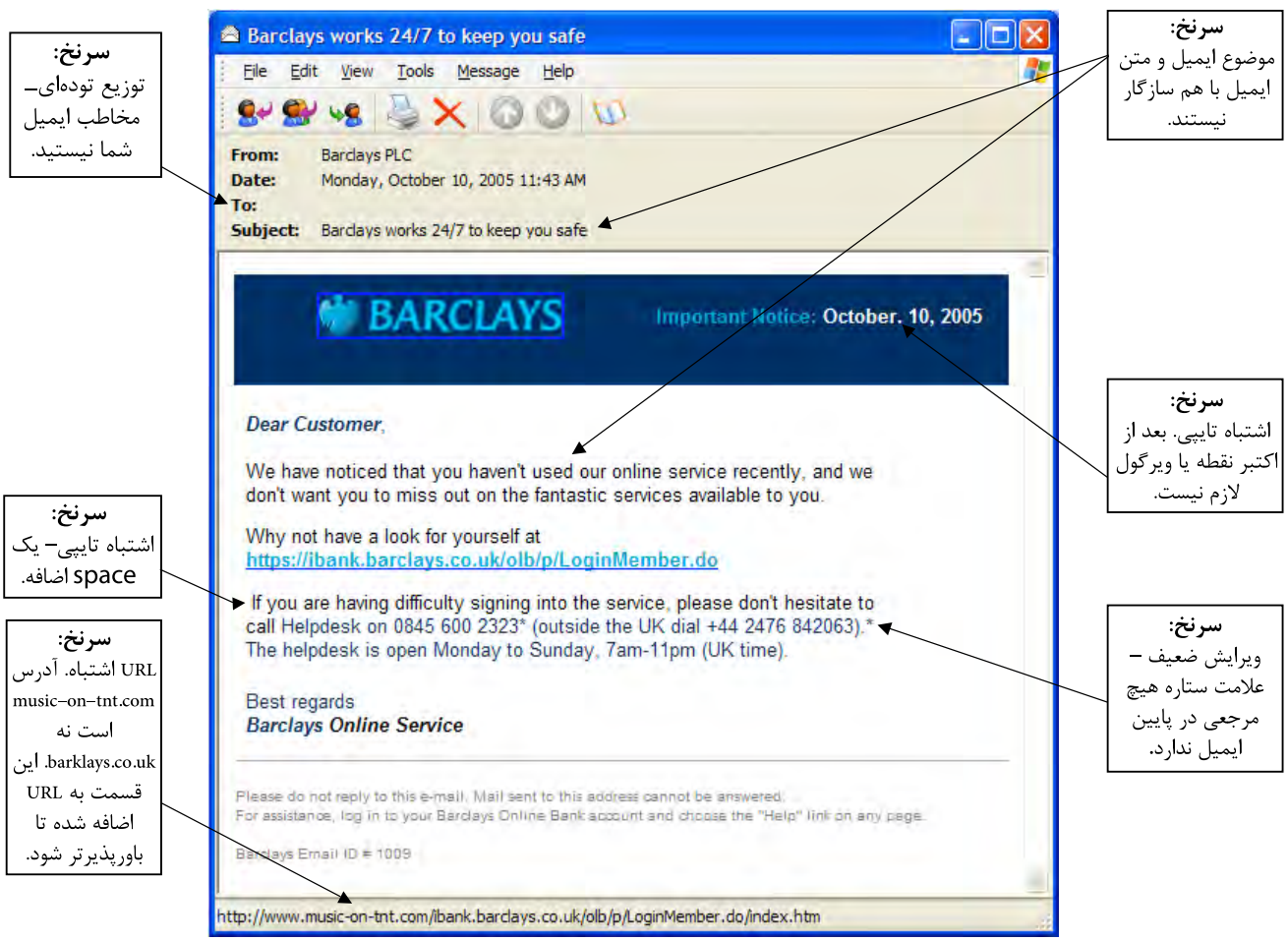


شن‌ماهی (Sandphish)

توضیح: شن‌ماهی، که در حفره‌های موجود در شن‌ها و گل‌های کف اقیانوس زندگی می‌کند، خیلی خوب می‌تواند خود را به مردگی بزند - هیچ وقت فکرش را هم نمی‌کنید که ممکن است سمی باشد.

رفتار: این موجود که به ظاهر کاملاً بی آزار است، اصلاً اینگونه نیست. شن‌ماهی معمولاً از شما می‌خواهد که برای خودتان کاری بکنید - به یک خدمت حفاظت از کارت اعتباری بپیوندید یا یک PowerSeller شوید. تمام سعی خود را کرده که از آن‌ها عبور کنید و بگذارید در همان حفره‌های کف اقیانوس باقی بمانند.

حقه: به نظر می‌رسد که فرستنده در حال ارائه‌ی یک خدمت به شماست و از شما می‌خواهد تا با کلیک روی لینکی که فیشینگ ارائه کرده است، از این مزایای این خدمت عالی استفاده کنید.

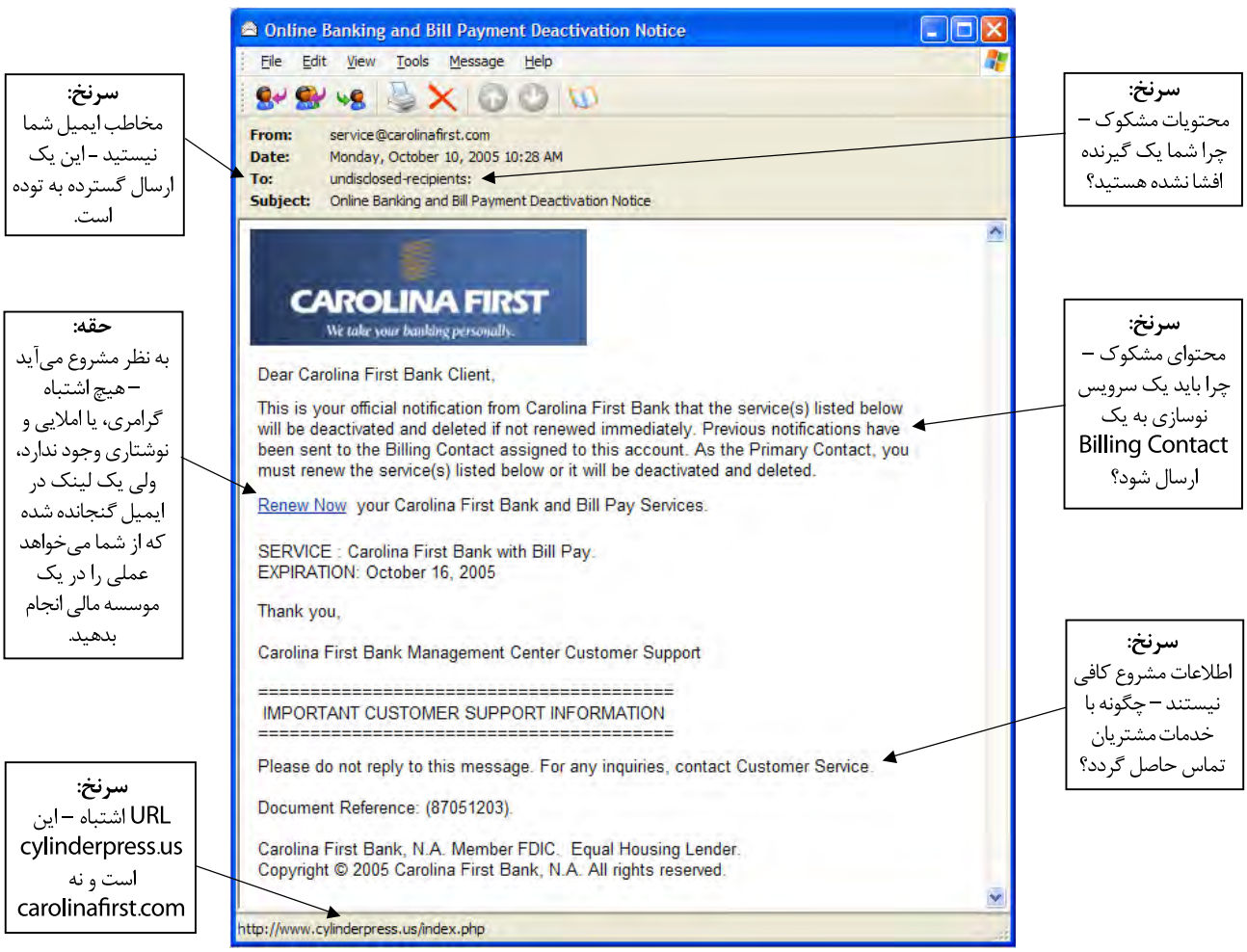


اردک‌ماهی (Walleye phish)

توضیح: در حالی که اردک‌ماهی ممکن است کسل‌کننده، ایمن و مشروع به نظر برسد - گول نخورید - دندان‌های تیزی دارد.

رفتار: این فیشینگ افراد را اینگونه فریب می‌دهد که ظاهراً از یک بانک یا موسسه اعتباری ارسال شده است. اردک‌ماهی مکرراً اطلاعات حساب، شماره‌های PIN عابرکارت‌ها، و دیگر اطلاعات حساس را از شما درخواست می‌کند که دسترسی به حساب‌های مالی شما را ممکن می‌سازند. برای مثال، «ما در حال ارتقا سیستم‌های خود هستیم و از شما می‌خواهیم که وارد سامانه شوید» یا «کارت اعتباری شما در سیستم ما منقضی شده است.» مراقب اردک‌ماهی و ادعاهای بی اساسش باشید.

حقه: ظاهر این نوع فیشینگ طوری است که می‌خواهد «به شما کمک کند» ولی اصولاً هدفش سرقت اطلاعات حساب شماست.

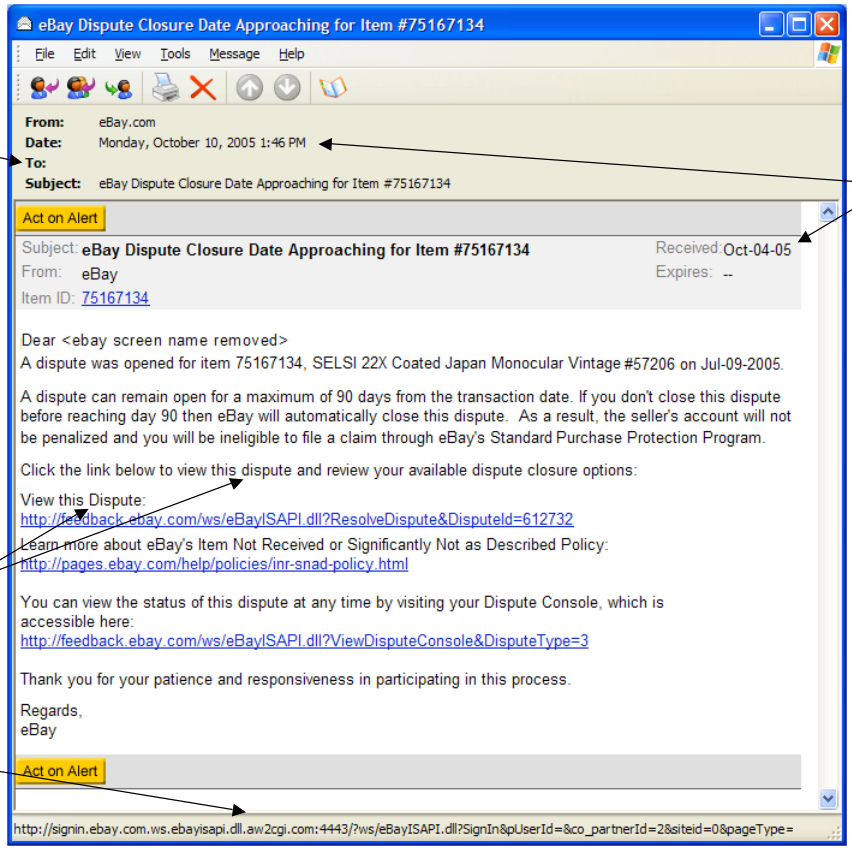


شمشیرماهی (Swordphish)

توضیحات: شمشیرماهی به خاطر رویکرد هدفمند و متمرکز خود به قربانیان معروف اند. این فیشینگ‌ها جنگجویان قدرتمندی هستند و تمایل دارند به تنهایی یا در گروه‌های کوچکی شنا کنند.

رفتار: شمشیرماهی‌ها بسیار تراکنش‌محور هستند و از فعالیت‌های «واقعی» در حساب شما، به عنوان ابزاری برای کمین کردن به منظور مشاهده‌ی واکنش استفاده می‌کنند. ویژگی شاخص شمشیرماهی این است که حاوی اطلاعاتی است که خاص شماست، مانند اسم شما، و برای خود شما ارسال می‌شود به جای اینکه توزیع توده‌ای شود. برای مثال، شمشیرماهی ادعا می‌کند که یک سپرده‌ی ۱۵۴،۸۵ دلاری در حساب شما منتظرتان است، و یا اینکه از شما می‌خواهد کاری انجام دهید زیرا که در یک مزایده آنلاین کسی پیشنهاد قیمتی بالاتری ارائه داده است. این حملات هدفمند می‌توانند کارساز باشند. اجازه ندهید این فیشینگ اطلاعات حساب شما را شکار کند.

حقه: این فیشینگ برای اینکه مشروع و سالم جلوه کند، از نام کاربری، نام عضویت و دیگر اطلاعات شخصی‌تان استفاده می‌کند. همچنین از یک تراکنش باورپذیر استفاده کرده و از شما می‌خواهد تا با استفاده از URL موجود در ایمیل اقدام کنید.



سرنخ:
نام عضویت یا نام کاربری شما در eBay

سرنخ:
تراکنشِ خاص – ولی آیا واقعاً شما روی یک این دوربین تلسکوپی ژاپنی پیشنهاد قیمت داده بودید؟ اصلن آیا برای این آیتم، وارد یک منازعه شده بودید؟

سرنخ:
ویرایش ضعیف – استفاده‌ی بی مورد از حروف بزرگ در اول کلمه.

سرنخ:
URL اشتباه – این ebay.com نیست، بلکه aw2cgi.com است. Ebay.com به ابتدای آن اضافه شده تا قانونی و مشروع جلوه کند.

سرنخ:
تاریخ گیج کننده – آیا تاریخ دهم اکتبر است یا چهارم اکتبر؟

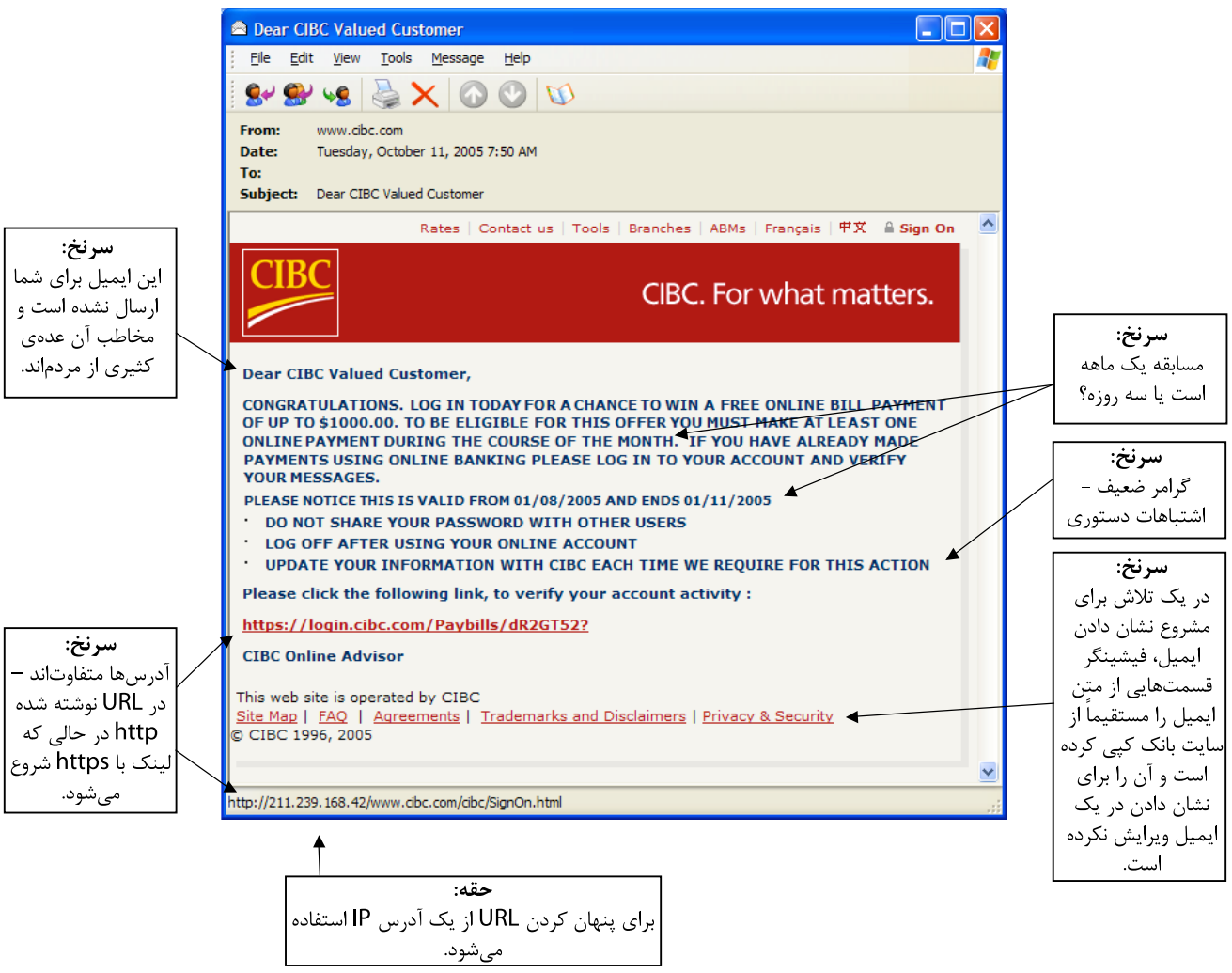
حقه:
به یک تراکنش خاص اشاره دارد، از شما یک واکنش خاص می خواهد، از اینکه کاری انجام ندهید شما را بیم می‌دهد. از شما می‌خواهد برای عمل کردن از لینک یا دکمه‌ی ارائه شده در ایمیل استفاده کنید.

ماهی قلابگیر (Anglerphish)

توضیحات: ماهی قلابگیر در آب‌های عمیق کمین می‌کند. یک نور آبی‌رنگ روشن به حالتی قلاب مانند جلوی دهان وی آویزان شده است تا قربانی به سوی آن جذب شده و در نهایت شکار شود. هنگامی که شکار به طعمه واکنش نشان داده و به سوی نور جذب می‌شود، ماهی قلابگیر آن را شکار می‌کند. مصون بمانید و از نور آبی فاصله بگیرید!

رفتار: ماهی قلابگیر اعلام می‌کند که شما برنده‌ی یک مسابقه یا قرعه‌کشی شده و برای ادعای جایزه خود باید اطلاعات شخصی خود را در اختیار ما قرار دهید. درسی که باید بگیرید این است که فریب طعمه اشتباهی را نخورید.

حقه: ماهی قلابگیر روی تمایل بشر به بردن یک قرعه‌کشی یا بدست آوردن چیزی بدون انجام دادن کاری متکی است. اگر فکر می‌کنید برنده شده اید، به بانک خود زنگ بزنید - روی لینک کلیک نکنید.



طوطی‌ماهی (Parrotphish)

توضیحات: طوطی‌ماهی یک فیشینگ بسیار خوش خط و خال است. بسیار جلب توجه می‌کند، از بیرون بسیار می‌درخشد که یادآور نورهای موجود در جشن‌هاست!

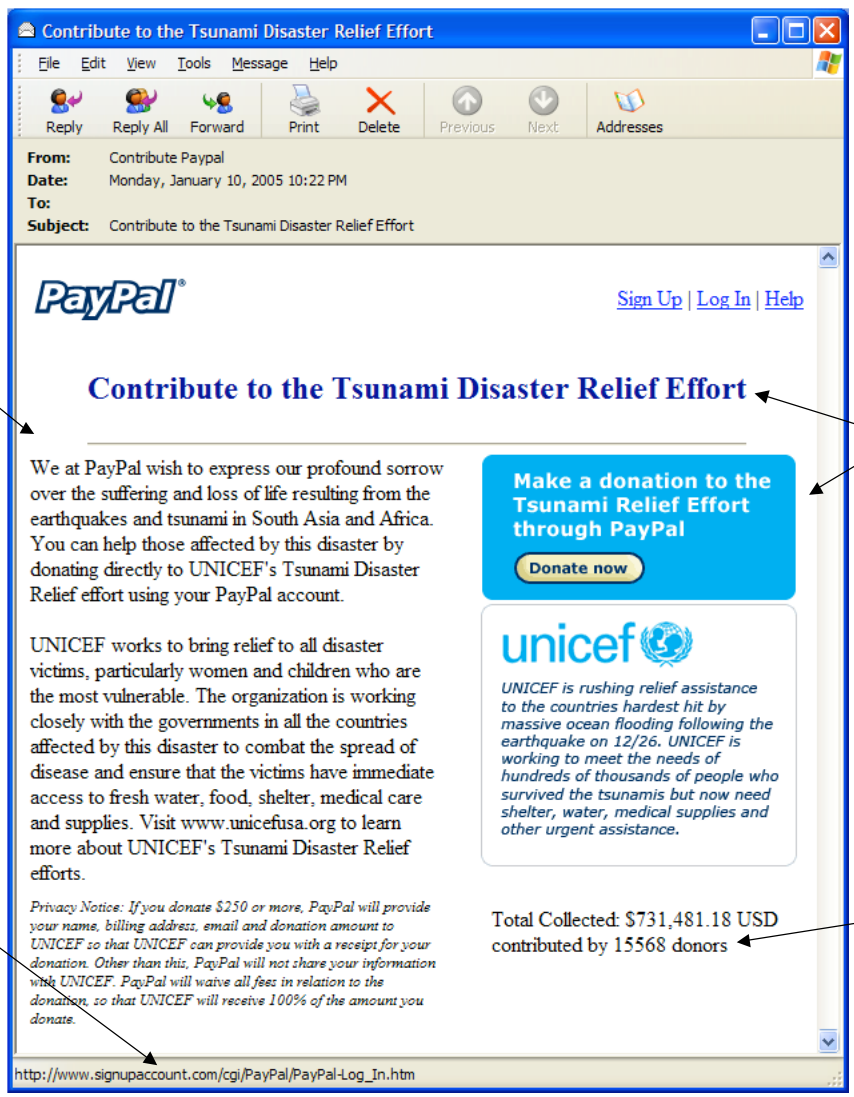
رفتار: این فیشینگ شکارهای خود را در رویدادهای فصلی یا ملی انتخاب می‌کند و از عواطف و سخاوت مربوط به این زمان‌ها سوء استفاده می‌کند. فریب زیبایی طوطی‌ماهی را نخورید زیرا اگر نزدیک به آن شنا کنید، دندان‌های تیزش از منابع شما یک گاز گنده می‌گیرد.

حقه: از تمایل شما به کمک به مردم سوء استفاده می‌کند، و «ثابت» می‌کند که دیگران هم کمک کرده‌اند.

سرنخ:
مخاطب آن شما نیستید.

حقه:
از نیاز ما به کمک کردن سوء استفاده می‌کند، نشان می‌دهد که دیگران هم کمک کرده‌اند.

سرنخ:
نام دامنه signupaccount.com است و نه PayPal.com. در واقع نام paypal بعد از نام دامنه اضافه شده است.



سرنخ:
بیشتر محتویات ایمیل از سایت‌های قانونی و مشروع کپی شده و درون ایمیل فیشینگ قرار داده شده‌اند.

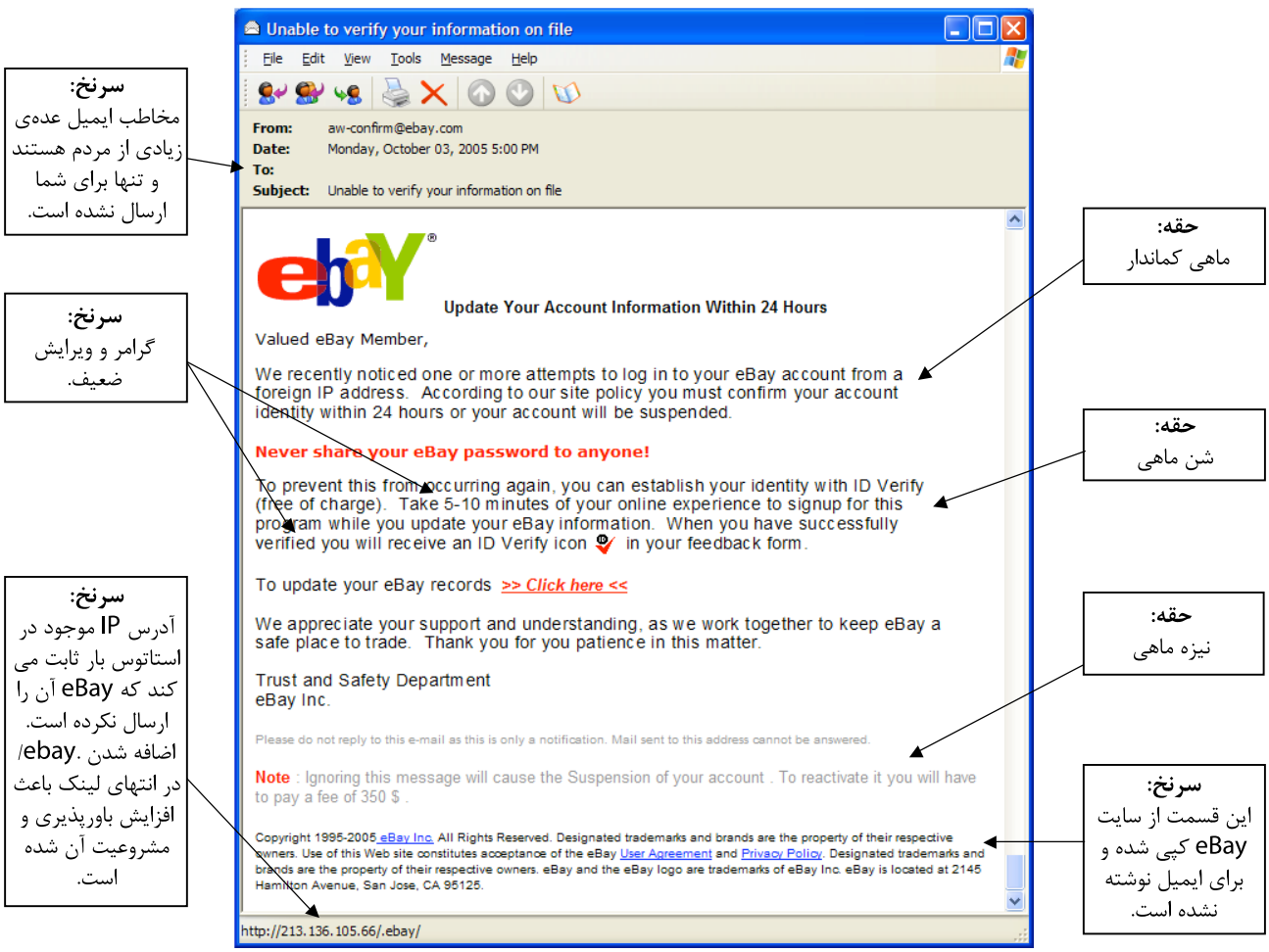
سرنخ:
ویرایش ضعیف - غلط املایی در کلمه‌ی donors

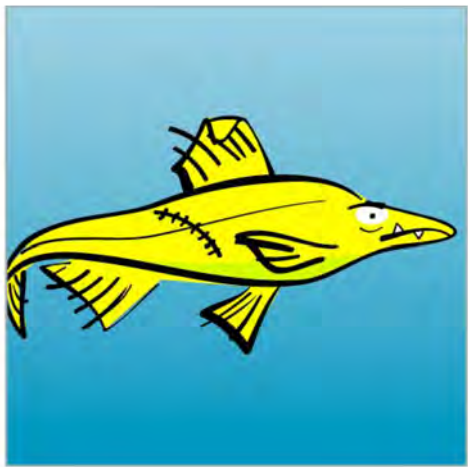
هشت‌پا (Octopus phish)

توضیحات: هشت‌پا به خوبی می‌تواند با رنگ‌ها و شکل‌های متفاوت رژه برود و دیگران را فریب دهد. این فیشینگ دست‌وپاهای زیادی در نواحی مختلف دارد تا قربانیان خود را به دام بیاندازد.

رفتار: این موجود روش‌های مختلف معرفی شده در فیشینگ‌های قبلی را با هم ترکیب می‌کند. برای مثال، یک هشت‌پا ممکن است نقش یک فرستنده‌ی قربانی را بازی کند، در حالی که در فصل تعطیلات، درخواست کمک مالی بکند. تهدیدی که این نوع فیشینگ به شما وارد می‌کند اثری خفه کننده است. مراقب باشید.

حقه: ترکیبی از تمامی حقه‌های فیشینگ‌های دیگر.



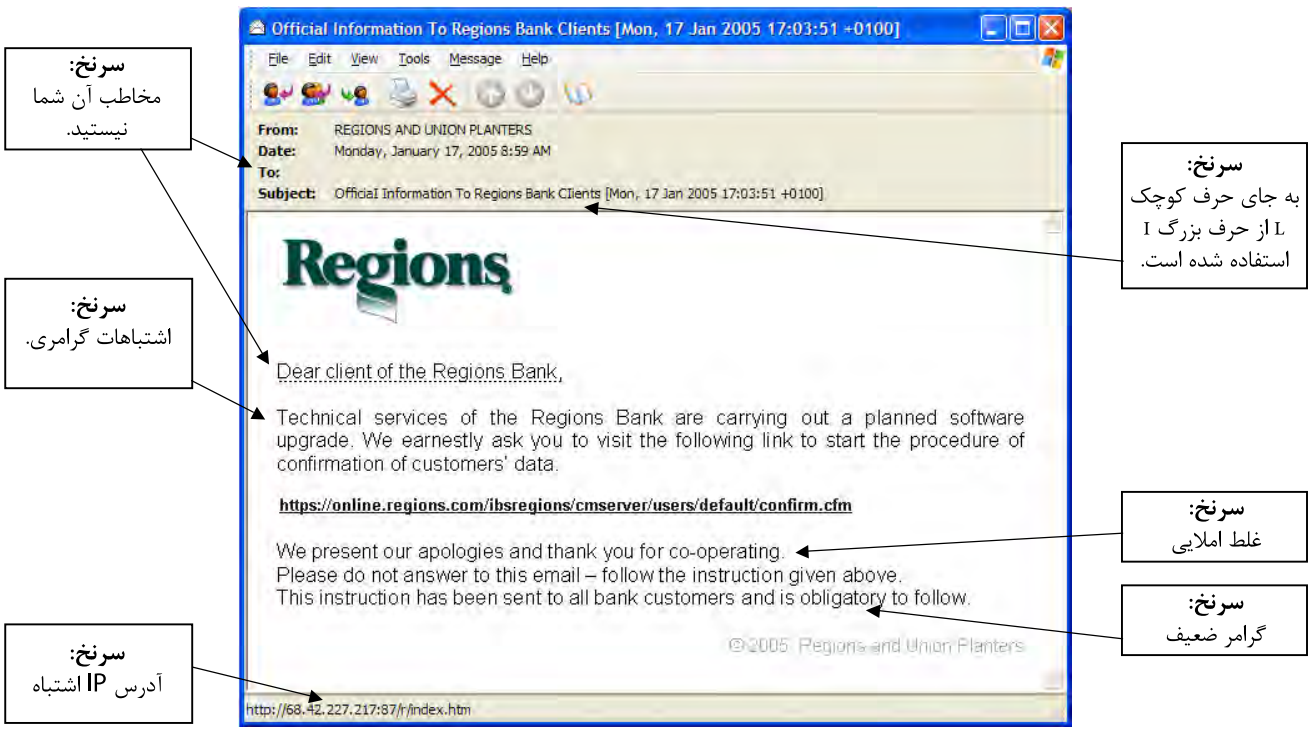


ماهی کپور (Bonytail phish)

توضیحات: ماهی کپور از کمیاب‌ترین نوع فیشینگ‌ها است و عضوی از خانواده ماهی‌های قنات است. این ماهی باله‌های بزرگی داشته و بدنی کاملاً ابتدایی و متعارف دارد؛ این نوع فیشینگ تقریبا منقرض شده است.

رفتار: اساساً، ماهی کپور می‌تواند هر نوع فیشینگی باشد، ولی بسیار بدون مهارت انجام شده است. این گونه جانوری در حال نابودی است، ولی این روزها نیز گاهاً می‌توان آن‌ها را با غلط‌های املایی واضح و اشتباهات گرامری مشاهده کرد.

حقه: حقه‌های آن قدیمی و شناسایی آن‌ها آسان است، مگر برای کسانی که بسیار ساده‌لوح‌اند!



چگونه از خود محافظت کنید؟

نکته۱:

اگر شما مشتری سازمانی نیستید که برای شما ایمیل فرستاده است، آن را نادیده بگیرید.
کلاهبرداران به تعداد کمی از مشتریان سازمان خاصی متکی هستند تا در دام تله‌های آن‌ها بیافتند.

نکته۲:

حتی اگر مشتری آن سازمان بودید، هرگز مستقیماً به یک ایمیل از طرف سازمان که اطلاعات شخصی یا مالی شما را درخواست کرده است جواب ندهید.
در عوض با استفاده از یک آدرس ایمیل یا شماره تماس که از مشروع بودن آن اطمینان دارید، اصالت درخواست را جویا شوید.

نکته۳:

هرگز از طریق ایمیل ارائه شده در لینک موجود در ایمیل وارد یک سایت نشوید.
در عوض یک مرورگر باز کرده و آدرسی که مطمئن هستید مشروع و سالم است را در آن وارد کنید. حتی از آن بهتر می‌توانیداز بوک‌مارک‌هایی که ساخته‌اید استفاده کنید.

نکته۴:

بعد از هر رسید، بیانیه‌های بانک و کارت اعتباری خود را چک کنید.
به دنبال هزینه‌ها و تراکنش‌هایی باشید که انتظارشان را نداشتید؛ حتی کوچکترین‌ها هم می‌توانند نشانی از دردسر باشند.

نکته۵:

اگر ناخواسته اطلاعات شخصی و مالی خود را افشا کرده اید، مراکز مربوطه را سریعاً در جریان قرار دهید.
بانک‌ها و موسسه‌های کارت‌های اعتباری با شما همکاری کرده تا اطلاعات شما بر علیه‌تان استفاده نشود.

نکته۶:

با روش‌های تجارت آشنا شوید تا ایمیل‌های کلاهبردارانه را شناسایی کنید.
دانش یک سلاح قدرتمند در جنگ علیه کلاهبرداران اینترنتی است.

نکته۷:

بروز باشید.
اطمینان حاصل کنید سیستم عامل شما و نرم‌افزارهای امنیتی اصلی شما، مانند ضدهرزنامه‌ها، ضدفیشینگ، ضدویروس و ضدجاسوس‌افزارها بروز هستند.

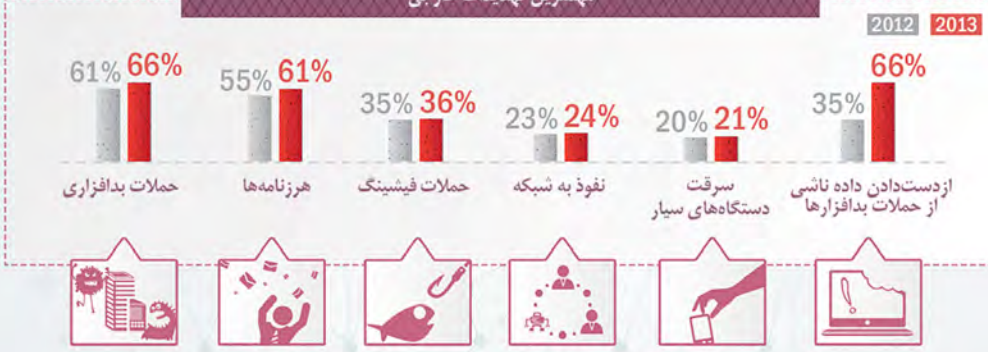
رویکرد کسب‌وکارها به امنیت فناوری اطلاعات در ۲۰۱۲-۲۰۱۳

کسب‌وکارهای کوچک (۱۰ تا ۹۹ کامپیوتر)
کسب‌وکارهای کوچک و متوسط (۱۰۰ تا ۱۵۰۰ کامپیوتر)
کسب‌وکارهای بزرگ (۱۵۰۰ کامپیوتر و بیشتر)

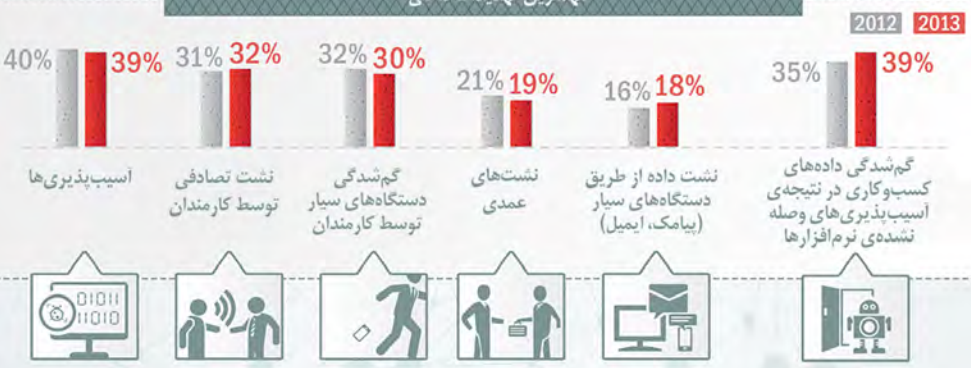
In 24 countries around the world

از چه کسانی سوال کردیم؟ ◄
مدیران اجرایی از ۲۸۹۵ شرکت

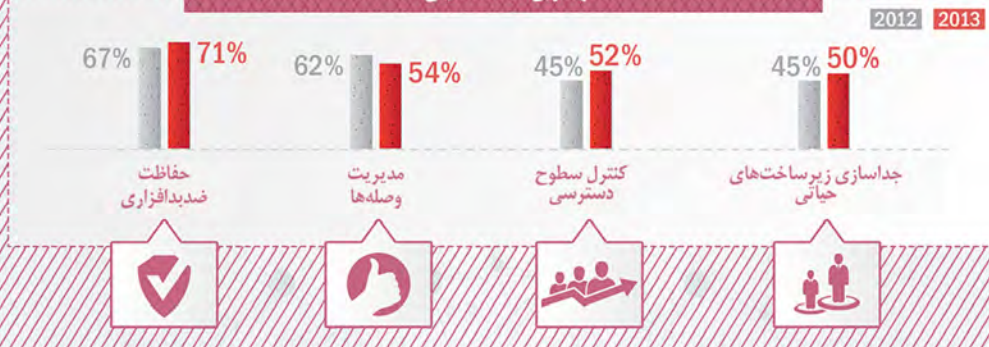
مهمترین تهدیدات خارجی



مهمترین تهدیدات داخلی



مهمترین اقدامات امنیتی



فزاینده‌ترین اقدامات امنیتی در ۲۰۱۳