امنیت کاربری فناوری اطلاعات

برگرفته از کتاب امنیت فناوری اطلاعات

تألیف:
جورج سادوســکای
جیمز اکس. دمپزی
آلــن گرینبرگ
باربارا جی. مک
آلــن شوارتز

ترجمه:
مهدی میردامــادی
زهـــرا شجـــاعی
محمدجواد صمدی

کلیات دوره امنیت کاربری فناوری اطلاعات (اکفا)

- کلیات امنیت سایبری
- بهداشت سایبری
- امنیت سایبری در سازمان‌ها
- امنیت در شبکه‌های اجتماعی
- مهندسی اجتماعی
- آشنایی با نهادهای متولی امنیت سایبری
- مفاهیم حقوقی فضای سایبری

کلیات امنیت سایبری

فضای سایبری

شبکه ای متصل به هم از زیر ساخت های فناوری اطلاعات است که اینترنت،شبکه های مخابراتی،سیستم های کامپیوتری،و پردازشگرها و کنترلگرهای داخلی صنایع مهم را شامل میشود[1].

کلیات امنیت سایبری

مشخصات فضای سایبری

فضای سایبری گسترده و بی حد ومرز است، و از نظر قانونی مبهم و از نظر شفاهی موجز و مختصر و در کل ،پیچیده و دست نیافتنی است.فضای سایبر باید در کنار عرصه های سنتی تر زمین ، هوا ، دریا ، فضا ، به عنوان ((پنجمین عرصه)) تلقی شود. اغلب مردم فکر میکنند که هکر ها ، مهارت و دانش بالایی دارند که میتوانند سیستم های کامپیوتری را هک کنند و نقاط آسیب پذیر را پیدا کنند. در حقیقت یک هکر خوب ، تنها باید نحوه کار سیستم کامپیوتری را بداند و نیز بداند که از چه ابزارهایی برای یافتن ضعف های امنیتی استفاده میشود[1] .

کلیات امنیت سایبری

- **امنیت فضای سایبری شامل سه عنصر پایه ای است[2] :**
  - محرمانگی
  - یکپارچگی
  - در دسترس بودن

کلیات امنیت سایبری[1]

- **محرمانگی:** به این معنا که اگر داده هایی که در فضای سایبری در حال انتقال هستند،توسط مهاجمین خوانده شوند و محرمانه بودن آن نقض شود.

- **یکپارچگی:** اگر در حین انتقال داده ها در فضای سایبری(به عنوان مثال در یک شبکه) اطلاعات توسط مهاجمین دستکاری شده و تغییر داده شوند(به آن چیزی اضافه یا از آن کم شود).

- **در دسترس بودن:** این نوع حملات با هدف خارج کردن منبع اطلاعاتی از سرویس به گونه ای که دیگر آن منبع قادر به ارائه سرویس به دیگران نبوده و نتواند تبادل اطلاعات درستی با کاربرانش داشته باشد ، انجام می شود .

کلیات امنیت سایبری

- برقراری امنیت در فضای سایبری ، به علت ماهیت فضای سایبری کار بسیار دشواری است، از فناوری سایبری بی تردید میتوان همانند ابزارهای جنگ متعارف، برای حمله به تشکیلات دولتی، نهادهای مالی، زیرساخت های انرژی و حمل و نقل ملی و روحیه عمومی استفاده کرد، فلذا ناامنی در فضای سایبری، صرفا شامل ناامنی در سیستم های اطلاعاتی نیست، بلکه شامل تمام زیرساخت هایی میشود که به نحوی با فناوری اطلاعات درارتباطند[3] .

کلیات امنیت سایبری

- حمله سایبری

به هر گونه اقدام غیر مجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دست یابی به اطلاعات سرمایه ملی سایبری مذکور انجام گیرد، حمله سایبری اطلاق می گردد[3] .

کلیات امنیت سایبری

آسیب پذیری سایبری[3]

چنانچه ضعف موجود در داخل سامانه سایبری موجب از بین رفتن سرمایه سایبری و یا اختلال در روند اجرای آن شود.

مخاطره سایبری

به احتمال بهره برداری یک تهدید سایبری از یک یا چند آسیب پذیری سایبری موجود به منظور تخریب، ایجاد اختلال، دسترسی غیر مجاز، افشای اطلاعات، دستکاری اطلاعات یا ممانعت از ارائه خدمات محسوب می شود.

کلیات امنیت سایبری

- **هکر:**
- دردهه ۱۹۷۰ واژه هکر به شخصی اطلاق می‌شد که در برنامه نویسی بسیار ماهروباهوش باشد . بعدها دردهه ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید به صورت ناشناس تبحر داشته باشد. امروزه بیشتر با هدف ترساندن هکرها، رسانه‌ها ومقامات مسئول مانند آژانس‌های دولتی وادارات پلیس، این واژه را به هرشخصی که مرتکب یک جرم مرتبط با فناوری شود، اطلاق می‌کنند[3] .

انواع نفوذ گران و بازیگران تهدید

گروه نفوذگران کلاه صورتی

- این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند.

گروه نفوذگران کلاه خاکستری

- اشخاصی هستند که حد وسط دو تعریف کلاه سفید و سیاه می‌باشند.

گروه نفوذگران کلاه سیاه

- اشخاصی هستند که وارد رایانه قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن بدافزار و غیره می‌پردازند.

گروه نفوذگران کلاه سفید

- هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند که در حقیقت متخصصین شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا کرده و به مسئولان گزارش می‌دهند.

انگیزه‌های تهدید

- تجاری
- مالی
- تلافی جویانه
- تفننی

کلیات امنیت سایبری

ویروس :

ویروس‌ها یا برنامه‌های خود همانندساز، برنامه‌هایی هستند که با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند ومعمولا از طریق یک دیسکت وگاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند.بعضی ویروسها ممکن است قادر به حمله به فایل‌های سیستم وذوب کردن مادربورد یک رایانه ، پاک کردن تمام داده‌های دیسک سخت وازکارانداختن رایانه باشند عنکبوت‌های موتورهای جستجووپالس‌های الکترومغناطیس که می‌توانند هارد سخت یک رایانه را ذوب کنند[2] .

بهداشت سایبری

طی چند سال اخیر ، سیستم هـای کـامپیوتری (رایانـه ، نـوت بـوک ، تلفن های هوشمند و ...) یکی از وسایل هایی بـوده اسـت کـه رشـد بسیاری در زندگی ما داشته به گونـه ای کـه در منـزل و محـل کـار زمان زیادی را با آن ها سپری کرده و اطلاعات مهمی را از قبیل نـام کاربری و رمز عبور حساب های بـانکی ، پسـت الکترونیکـی و حسـاب هـای شخصـی در صـفحات مجـازی و ... را بـر روی آن نگهـداری میکنیم که در صورت عدم افزایش امنیت این نوع سیستم هـا باعـث سوءِاستفاده برخی از افراد از نقاط ضعف سیستم جهت انجام کارهای خرابکارانه ی خود می گردد[2] .

بهداشت سایبری

عدم اگاهی از نحوه پیکربندی و یا راه های نفوذ هکرها به سیستم های کامپیوتری یکی از اصلی ترین دلایل سرقت اطلاعات شخصی بسیاری از افرادی است که نا آگاهانه و یا بدون توجه به یک سری از نکات ابتدایی از سیستم های کامپیوتری استفاده می کنند[2] .

بهداشت سایبری[2]

راه‌های ایجاد امنیت در سیستم‌های خانگی و اداری

- نصب نسخه اصلی:
  - آنتی ویروس
  - نرم افزار ضد جاسوسی
- به روز رسانی مستمر نرم افزارها
- امنیت رمز عبور
- ذخیره‌سازی فایل های مهم و حساس در رسانه‌های قابل حمل مثل کول دیسک‌ها و سی دی و ...
- رمز نگاری پیشرفته پوشه ها و فایل‌ها

بهداشت سایبری[2]

راه‌های ایجاد امنیت در سیستم‌های اداری

- ✓ راه اندازی شبکه داخلی یا اینترانت
- ✓ ذخیره سازی اطلاعات حساس و مهم کاری بر روی حافظه های جانبی
- ✓ حفاظت فیزیکی از حافظه های جانبی
- ✓ بخش بزرگی از امنیت اطلاعات مهم و محرمانه در محیط کار مثل شبکه های کامپیوتری، امنیت نرم افزار و بانک اطلاعاتی و... بر عهده مسئولین IT است.
- ✓ حفاظت فیزیکی سیستم های اداری با حراست ادارات می باشد.
- ✓ باز نکردن نامه ها و ایمیل های دریافتی از منابع ناشناس
- ✓ خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه
- ✓ قطع اتصال به اینترنت در مواقع عدم استفاده
- ✓ گرفتن منظم وصله های امنیتی Patches
- ✓ حصول اطمینان از آگاهی کاربران از نحوه برخورد با کامپیوترهای آلوده
- ✓ بررسی مرتب میزان دریافت و ارسال اطلاعات

بهداشت سایبری

تهدیدات مربوط به امنیت سیستم[2]

Virus

برنامه ای که با کپی کردن خود در برنامه های دیگر، سکتورهای بوت سیستم یا داکیومنت ها تکثیر شده و فایل های کامپیوتر و نیز اپلیکیشن ها را تغییر می دهد و یا به آن ها آسیب می رساند

Worm

یک ویروس خود تکثیر که فایل ها را تغییر نمی دهد اما در حافظه کامپیوتر مستقر شده و خود را تکثیر می نماید

Backdoor

یک شیوه غیرمجاز برای دسترسی به سیستم و دور زدن مکانیزم های امنیتی آن

Rootkit

مجموعه ای از برنامه ها یا ابزارها که دسترسی به سطح روت را در سیستم فراهم می کنند

Trojan

برنامه ای که مجاز به نظر می رسد اما پس از اجرا اقدامات مخرب انجام می دهد

Logic Bomb

برنامه ای که یک ویروس یا کرم را منتشر می کند

جاسوس افزار

جاسوس افزارها شامل تروجان‌ها و سایر نرم‌افزارهای مخرب هستند که بدون اطلاع کاربر اطلاعات شخصی وی را از سیستم سرقت می‌نمایند. مانند: کی لاگر

کی لاگر

کی لاگر یک دستگاه سخت افزاری یا یک برنامه نرم افزاری کوچک است که هر کلیدی را که بر روی صفحه کلید کاربر فشرده می‌شود ثبت می‌کند.

کرک پسورد

کرک پسورد فرآیند شناسایی یا بازیابی یک پسور ناشناخته یا فراموش شده است.

بهداشت سایبری

پخش بدافزار[2]

بدافزار چیست؟

- بدافزارها یا Malware ها برنامه‌های کوچک و البته مخربی هستند که می‌توانند اطلاعات شما را نابود کنند یا در کار با رایانه اختلال ایجاد کنند.
- بدافزارها معمولا برای اهداف جاسوسی و سرقت اطلاعات تنظیم می‌شوند و می‌توانند هویت کاربران را نیز در خطر قرار دهند.

از طریق پیوست‌های ایمیل

ایمیل‌های دارای پیوست ممکن است حاوی بدافزار باشند.

با کلیک بر روی پیوست یک برنامه مخرب بر روی کامپیوتر نصب می‌گردد.

از طریق کارت حافظه‌های USB

ویرویس یک فایل autorun.inf ایجاد می‌کند که یک فایل فقط خواندنی و پنهان است.

زمانی که کاربر فایل‌های درون USB را باز می‌کند autorun.inf اجرا شده و فایل‌های وردپرس را در سیستم کپی می‌کند.

از طریق سایت‌های آلوده

بازدید از سایت‌های آلوده ممکن است منجربه نصب نرم‌افزارهای مخرب (که به منظور سرقت اطلاعات طراحی شده‌اند) بر روی کامپیوتر کاربر شود.

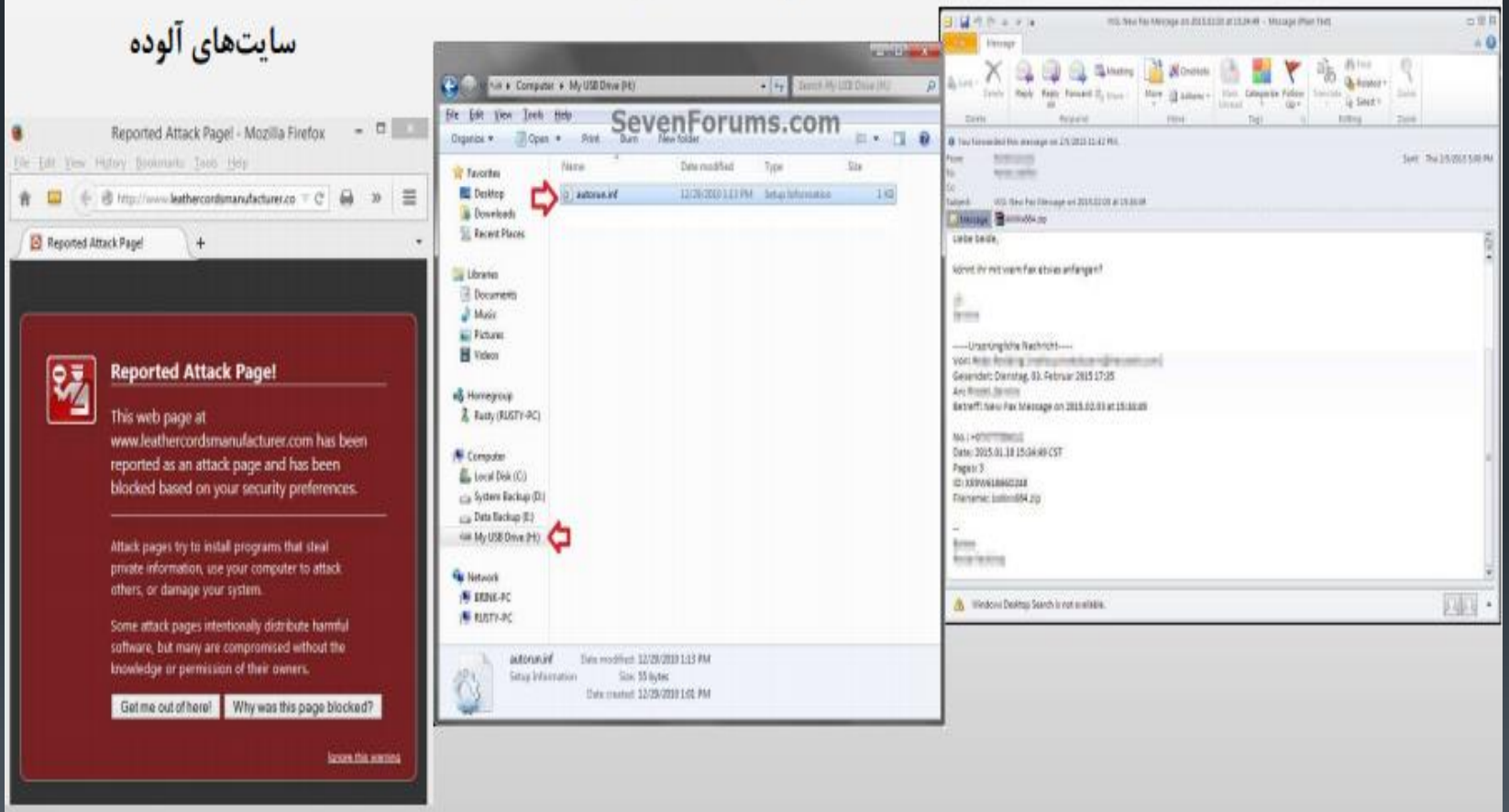
بهداشت سایبری

پخش بدافزار

پیوست‌های ایمیل

کارت حافظه‌های USB

سایت‌های آلوده



بهداشت سایبری

پخش بدافزار

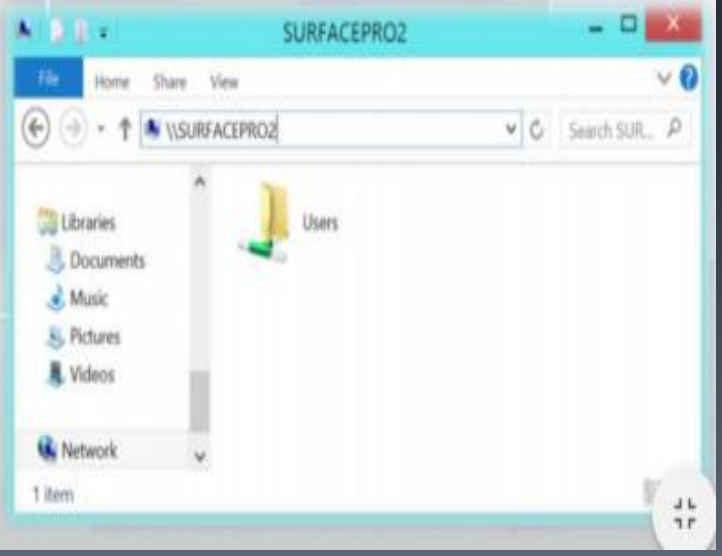
از طریق پوشه‌های اشتراک گذاری شده

بدافزار ممکن است از طریق اشتراک‌گذاری‌های شبکه پخش شود.

بدافزار ممکن است با کپی نمودن خود در پوشه‌های به اشتراک گذاشته شده گسترش یابد.

از طریق کدک

اگر کاربری بخواهد یک پلیر برای تماشای ویدئو دانلود و نصب نماید، کدک ممکن است یک برنامه مخرب باشد که بر روی سیستم دانلود می‌شود.



بهداشت سایبری

پخش بدافزار

از طریق دانلودها

دانلود نرم افزار، آهنگ، عکس و ویدئو از سایت‌های نامعتبر ممکن است منجربه دانلود یک فایل مخرب آلوده به ویروس، کرم، تروجان و غیره گردد.

اپلیکیشن‌های مخرب زیادی در اینترنت وجود دارند که با جلات تحریک کننده می‌توانند کاربران را برای دانلود وسوسه کنند.

از طریق آنتی ویروس جعلی

آنتی ویروس ۲۰۰۹ یک آنتی ویروس جعلی است که وانمود به اسکن کردن سیستم نموده و ویروس‌هایی را نشان می‌دهد که وجود ندارند.

با کلیک بر روی دکمه Register یا Scan بدافزار بر روی سیستم دانلود می‌شود.

بهداشت سایبری

پخش بدافزار[2]

اشتراک گذاری فایل peer-to-peer

- ✓ امکان به اشتراک گذاری موسیقی، تصاویر، داکیومنت‌ها و برنامه‌های نرم‌افزاری بین دو کامپیوتر را از طریق بستر اینترنت فراهم می‌آورد.
- ✓ فایل‌های به اشتراک گذاشته شده ممکن است حاوی خطرات امنیتی مانند ویروس، جاسوس افزار و سایر نرم‌افزارهای مخرب باشند.
- ✓ مهاجمان می‌توانند بدافزار را به عنوان یک اپلیکیشن مفید جلوه دهند.

بهداشت سایبری

پخش بدافزار[2]

نشانه‌های وجود یک بدافزار در رایانه:

- ✓ پاپ‌آپ‌ها (Pop-up)
- ✓ از کار افتادن ناگهانی سیستم
- ✓ فعالیت مشکوک هارد دیسک
- ✓ کمبود فضا روی هارد دیسک
- ✓ فعالیت غیرطبیعی شبکه
- ✓ تعویض صفحه نخست مرورگر، باز شدن سایت‌ها به صورت ناخواسته
- ✓ پیغام‌های غیرطبیعی یا باز شدن ناخواسته نرم‌افزارها
- ✓ کار نکردن نرم‌افزارهای امنیتی
- ✓ دریافت پیغام‌های غیرعادی توسط دوستانتان

بهداشت سایبری

دستورالعمل های امنیتی ویندوز[2]

- زمانی که سیستم بلااستفاده است آن را قفل نمایید
- ایجاد رمز عبور قوی
- غیرفعال نمودن حساب کاربری Guest
- قفل نمودن اکانت بعد از چندین بار ورود ناموفق
- حساب کاربری Administrator را تغییر نام دهید
- غیرفعال نمودن منوی Start up
- اعمال وصله های امنیتی نرم افزارها
- استفاده از فایروال ویندوز
- استفاده از NTFS
- استفاده از رمزگذاری فایل سیستم ویندوز
- فعال نمودن Bitlocker
- غیرفعال نمودن سرویس های غیرضروری
- متوقف نمودن پردازش های غیرضروری
- پیکربندی سیاست های ممیزی (Audit Policy)
- مخفی نمودن فایل ها و پوشه ها
- غیرفعال نمودن اشتراک گذاری فایل
- استفاده از کنترل حساب کاربری ویندوز(UAC)
- پیاده سازی مکانیزم های پیشگیری از بدافزار

بهداشت سایبری

دستورالعمل های امنیتی ویندوز

توصیه‌هایی در رابطه با به روزرسانی

- همیشه سیستم عامل و برنامه‌های را با آخرین وصله‌های امنیتی وصله نمایید.
- وصله‌های امنیتی را فقط از منابع معتبر دانلود کنید، ترجیحا از سایت‌های معتبر عرضه کننده‌ی نرم‌افزار مانند مایکروسافت.
- تنظیمات را به گونه‌ای تنظیم نمایید که هشدار عرضه کنندگان در رابطه با آسیب‌پذیری‌ها برای شما ارسال شود.
- فایل‌های اجرایی را که از منابع مشکوک هستند باز نکنید.
- وصله‌های امنیتی را از طریق ایمیل ارسال نکنید.
- برای نصب آسانتر به روز رسانی‌ها از ابزارهای مدیریت پچ استفاده نمایید.

بهداشت سایبری

امنیت رمز عبور[2] [3]

- طول رمزهای عبور خود را بیشتر از ۸ کاراکتر (حرف) انتخاب کنید. **aminbahrami**
- درون رمز عبور خود، هم از حروف بزرگ و هم از حروف کوچک استفاده کنید. **AminBahrami**
- درون رمز عبور خود، از اعداد نیز استفاده کنید. **aminbahrami1236**
- درون رمز عبور خود، از علائم انگلیسی مانند نقطه، فاصله، اعشار، و علائم دیگر مانند ~,!,@,#,$,%,^,&,*,_,=,+,/,\,|,?,>,<,...» استفاده کنید. **m1n 8ahraml@**
- درون رمز عبور خود، از حروف اضافه انگلیسی «,,:,;,',"» و ...» استفاده کند. **amin.:.bahrami;**
- درون رمز عبور خود، از انواع پرانتز ({,},(,),[,]) استفاده کنید. **amin][bahrami]**

بهداشت سایبری

امنیت ایمیل[2] [3]

سیستم‌های مختلف ایمیل چگونه کار می‌کنند؟

- ایمیل یک روش تبادل پیام‌های دیجیتالی از یک فرستنده به یک یا چند گیرنده است.
- شرکت‌هایی مانند Microsoft، Yahoo، Google، AOL از حساب‌های ایمیل رایگان خود استفاده می‌کنند.
- حساب‌های ایمیل، از هر مرورگر وب یا کلاینت ایمیل مانند Microsoft Outlook، Mozilla Thunderbird و غیره قابل دسترسی است.

بهداشت سایبری

امنیت ایمیل

اگر امن‌سازی صورت نگرفته باشد، ایمیل‌های فرستاده یا دریافت شده می‌تواند جعل یا توسط دیگران خوانده شود.

ایمیل‌های ناامن، به مهاجمان اجازه می‌دهند تا به **اطلاعات شخصی و حساس کاربر** دسترسی پیدا کنند.

ارتباط از طریق ایمیل به طور **۱۰۰ درصد** امن نیست.

لازم است که ایمیل‌ها برای **ارتباطات امن** و **حفاظت از حریم خصوصی**، ایمن شوند.

ایمیل‌ها یکی از منابع **ویروس‌ها** و برنامه‌های مخرب هستند.

بهداشت سایبری

امنیت ایمیل

تهدیدات امنیتی ایمیل [2]

Spamming

- کاربر ممکن است ایمیل‌های اسپمی را دریافت کند که حاوی نرم‌افزارهای مخرب باشد که به مهاجمین اجازه می‌دهد تا کامپیوتر کاربر را کنترل کند.

ایمیل Hoax/Chain

- ممکن است کاربر ایمیل‌های جعلی دریافت کند که شامل اطلاعات اشتباهی است که به او می‌گوید نامه‌ای را ارسال کند.

هدایت کاربر به یک آدرس مخرب

- ایمیل‌ها ممکن است حاوی لینک به سایت‌های مخرب یا دارای مطالب مربوط به pornographic باشند.

فیشینگ

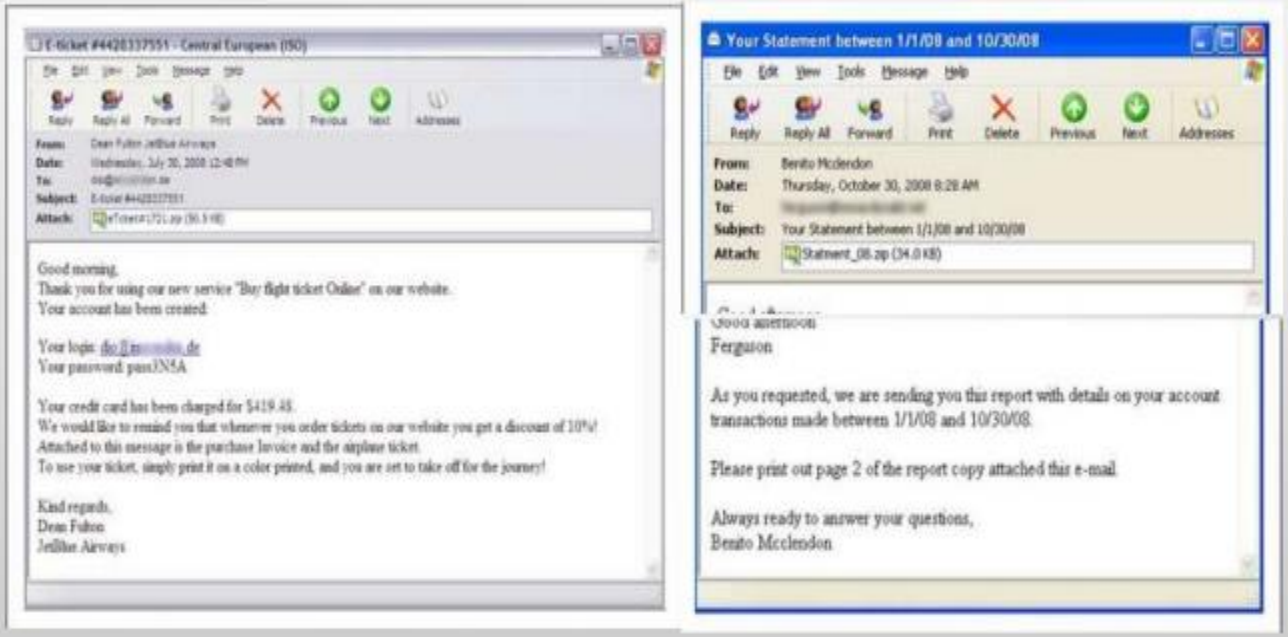
- ایمیل‌های فیشینگ قربانیان را برای ارائه‌ی اطلاعات شخصی فریب می‌دهند.

پیوست‌های مخرب ایمیل

- فایل‌های ضمیمه ممکن است حاوی یک ویروس تروجان، کرم‌های keylogger و... باشد و باز کردن چنین پیوست‌هایی کامپیوتر را آلوده می‌کند.

پیوست‌های مخرب ایمیل [2]

- پیوست‌های ایمیل تهدیدات امنیتی عمده‌ی ایمیل هستند، زیرا آنها ساده‌ترین و قویترین راه‌ها را برای حمله به یک کامپیوتر، به مهاجمان ارائه می‌دهند.
- بیشتر پیوست‌های مخرب، یک ویروس، تروجان، نرم‌افزار جاسوسی یا هر نوع دیگر از بدافزار را نصب می‌کنند که به زودی شما آنها را باز می‌کنید.



بهداشت سایبری

امنیت ایمیل

پیوست های ایمیل: هشدارها [2]

پیوست‌های حاوی فایل‌هایی با **پسوندهای مشکوک و ناشناخته** باز نکنید. به عنوان مثال: *.exe, *.vbs, *.bat, *.ini, *.bin, *.com, *.pif, *.zzx

هرگز پیوست‌های ایمیل ارسال شده از منابع غیرقابل اعتماد را باز نکنید.

بررسی کنید که ایمیل از یکی از **مخاطبین** شما فرستاده شده است.

بررسی کنید که آیا **موضوع ایمیل** با **نام پیوست** هماهنگی دارد یا خیر.

قبل از باز کردن، تمام پیوست‌ها را **ذخیره و اسکن** کنید.

بررسی کنید که آیا ایمیل از یک **منبع قابل اعتماد** دریافت شده است یا خیر

بهداشت سایبری

امنیت ایمیل

Spamming [2]

- استفاده از سیستم‌های ایمیل برای ارسال توده پیام‌های ناخواسته، بدون در نظر گرفتن صندوق‌های پستی کاربران است.
- ایمیل‌های اسپم ممکن است حاوی برنامه‌های کامپیوتری مخرب مانند ویروس‌ها و تروجان‌ها باشند.
- طبق گفته‌ی سیمانتک، اسپم ۸۹.۱ درصد از کل ترافیک ایمیل را تشکیل می‌دهد.

بهداشت سایبری

امنیت ایمیل

راه‌های مقابله با Spamming[2]

- هرگز لینک‌های موجود در پیام‌های اسپم را دنبال نکنید.
- از ابزارهای آنتی اسپم یا فیلتر اسپم کلاینت ایمیل استفاده کنید.
- از باز شدن پیام‌های اسپم جلوگیری کنید (مرتب شده توسط فیلترهای اسپم).
- هنگام ارسال پیام به هر انجمن عمومی، از یک آدرس ایمیل متفاوت استفاده کنید.
- برای ثبت‌نام در هر وب‌سایت، از آدرس ایمیل رسمی استفاده نکنید.
- ایمیل‌های اسپم مشکوک را گزارش کنید.

بهداشت سایبری

امنیت ایمیل

ابزار آنتی اسپم SPAM fighter [2]

این ابزار از تمام حساب های ایمیل در یک کامپیوتر در برابر "فیشینگ"، سرقت هویت و دیگر فریب های ایمیل محافظت می کند.

بهداشت سایبری

امنیت ایمیل

روش‌های امنیتی ایمیل

- ایجاد و استفاده از پسورد قوی
- تهیه آدرس ایمیل جایگزین برای بازیابی ایمیل
- آخرین لاگین را بررسی کنید
- از Https برای اتصال به مرورگر استفاده کنید
- گزینه‌های Singed In/ Remember Me, Keep Me را غیرفعال کنید یا انتخاب نکنید
- پیوست‌ای ایمیل را جهت یافتن نرم افزارهای مخرب اسکن کنید
- قابلیت پیش نمایش را خاموش کنید و تنظیمات دانلود را در کلاینت‌های ایمیل تغییر دهید
- فیلتر ایمیل کم اهمیت را در کلاینت‌های ایمیل ایجاد کنید
- پیام‌های ایمیل خود را به صورت دیجیتالی امضا کنید
- با استفاده از فیلترها، از ایمیل‌های ناخواسته جلوگیری کنید

بهداشت سایبری

امنیت ایمیل

ابزارهای امنیتی

Comodo AntiSpam
http://www.comodoantispam.com

McAfee SpamKiller
http://us.mcafee.com

Netcraft Toolbar
http://toolbar.netcraft.com

Comodo Email Certificate
http://www.comodo.com

PhishTank SiteChecker
https://addons.mozilla.org

Mirramail Secure Email
http://www.mirrasoft.com

Spamihilator
http://www.spamihilator.com

Encryptomatic MessageLock
http://www.encryptomatic.com

بهداشت سایبری

امنیت ایمیل

خلاصه

- Email (electronic mail) یک روش تبادل پیام‌های دیجیتال از یک فرستنده به یک یا چند گیرنده است.
- فایل‌های ضمیمه (پیوست‌ها) می‌توانند حاوی برنامه‌های مخرب باشند، که باز کردن چنین پیوست‌هایی می‌تواند کامپیوتر را آلوده کند.
- Spamming فرایند اشغالکردن صندوق ورودی کاربر با ایمیل‌های ناخواسته و بی ارزش است.
- Hoaxes هشدارهای دروغین با ادعای گزارش‌های مربوط به یک ویروس غیرواقعی هستند.
- پاک کردن Cache، پسوردها و history مرورگر را فراموش نکنید.
- تنظیمات تلفن همراه را فقط برای دانلود header ایمیل‌ها در نظر بگیرید نه برای تمام ایمیل
- امضاهای دیجیتال برای تایید هویت فرستنده یک پیام یا امضا کننده یک داکیومنت، استفاده می‌شوند.
- ابزارهای امنیتی ایمیل از پسوردها و خروج خودکار از حساب‌های کاربردی ایمیل، محافظت می‌کنند.

بهداشت سایبری

امنیت ایمیل

چک لیست امنیت ایمیل

- هنگام ارسال ایمیل به تعدادی از گیرندگان، از گزینه Bcc استفاده کنید.
- هرگز پسورد خود را در مرورگر وب ذخیره نکنید.
- پیام‌ها را براساس الویت، موضوع، تارخ، فرستنده و دیگر موارد مرتب کنید. این کار به شما در جستجوی ایمیل‌ها کمک می‌کند.
- از ارسال اطلاعات محرمانه، حساس، شخصی و طبقه‌بندی شده در ایمیل‌ها اجتناب کنید.
- صندوق وردوی خود را مرتبا پاک کنید.
- پوشه‌هایی را ایجاد کنید و ایمیل‌ها را براساس خانواده، دوستان، کار و غیره به آنها انتقال دهید.
- ایمیل‌هایی را که ارسال می‌کنید، به صورت دیجیتالی امضا کنید.

بهداشت سایبری

امنیت ایمیل

چک لیست امنیتی برای بررسی ایمیل‌ها در موبایل

- تنظیمات موبایل برای دانلود Header ایمیل‌ها در نظر بگیرید نه برای تمام ایمیل
- فایل‌های پیوست بزرگ را از طریق موبایل، ارسال و باز نکنید.
- لینک‌هایی که توسط ایمیل یا پیام‌های متنی فرستاده شده‌اند، دنبال نکنید.
- یک آنتی ویروس موبایل نصب کنید و آن را آپدیت نگه دارید.
- گزینه نمایش تصاویر را در مرورگر موبایل خود غیرفعال کنید.
- برای کاهش اندازه ایمیل، آنها را یک متن ساده ارسال کنید.
- فایل‌های مهم را به صورت Zip ارسال کنید.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

اصولا برقراری امنیت سایبری در سازمان ها به تمامی کاربران مرتبط می‌باشد و در واقع محافظت از شرکت و کاربران آن در برابر نشت اطلاعات، فقط بر عهده کارشناسان عملیات امنیتی و بخش فناوری اطلاعات نیست و از هیئت مدیره گرفته تا کارمندان رده‌ی پایین، همه در این امر نقش مهمی را ایفا می‌کنند. ذهنیتی که افراد را متقاعد می‌کند که در حفاظت و نگهداری شرکت در برابر رفتار مخرب نقش مهمی دارند، به آگاهی همه‌ی افراد از خطرات روزمره و دانستن اقداماتی که به این خطرات مرتبط اند نیاز دارد[1] .

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

اهداف

1. آشنایی با اهمیت حفاظت از اطلاعات سازمان
2. آشنایی با حملات سایبری در سازمان ها
3. آشنایی با نحوه جلوگیری و مقابله با حملات سایبری
4. آشنایی با نحوه حفاظت از سیستم های درون سازمانی
5. امنیت شبکه های اجتماعی

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- اطلاعات عنصری حیاتی است که بقای سازمان ها به شدت به آن وابسته است و نیازمند راهکارهای حفاظتی مناسب؛ جهت جلوگیری از تخریب، دستکاری، حذف و یا ایجاد وقفه در خدمات است.
- گسترش روز افزون تهدیدات و افزایش حملات سایبری به سازمانها در سالهای اخیر، نشان دهنده آن است که شیوه‌های دفاع فعلی در برابر این تهدیدات دیگر جوابگو نیست و سازمانها نیازمند بکارگیری تدابیر اصولی تر در این حوزه هستند.
- **خسارات جبران‌ناپذیر ناشی از وجود یک حفره یا مشکل امنیتی در سازمان ها:**
  - ✓ از دست دادن اعتبار فعلی سازمان در میان رقبا
  - ✓ کاهش درآمدهای سازمانی
  - ✓ افزایش هزینه‌های سازمانی
  - ✓ سلب اعتماد مشتریان و سرمایه‌گذاران و حتی کارمندان
  - ✓ کاهش مشتریان سازمان

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

برخی از عوامل تهدیدکننده اطلاعات در سازمان‌ها [1]

تهدیدات نرم‌افزاری

- نفوذ به فایروال‌ها
- بدافزارها (ویروسها، تراواها، کرمها)
- انتشار غیرمجاز یا تخریب داده‌ها
- جاسوسی سازمان یافته به وسیله ابزارهای دیجیتالی.

تهدیدات فیزیکی

- بلایای طبیعی (آتشسوزی، زلزله، و...)
- دزدی
- تخریب
- تداخل‌های فیزیکی
- تخریب شبکه
- جاسوسی سازمان‌یافته

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

برای ارتقاء سطح امنیت در سازمان‌ها مراحل زیر پیشنهاد می‌شود [2]

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

اقداماتی برای پیاده‌سازی راه‌کارهای امنیتی مقرون به صرفه و سیستم امنیتی پویا [1]

ایجاد مراکز امداد جهت حملات سایبری احتمالی

استفاده از نرم‌افزارهای کاربردی جهت هر چه بیشتر سیستمی کردن امور و کاهش خطاهای انسانی

مدیران و کارمندان به طور پیوسته آموزش‌های امنیتی را دریافت کنند.

با استفاده از سیستم مدیریت امنیت اطلاعات (ISMS)، یک سری کنترل‌ها و محدودیت‌ها برای دسترسی افراد مختلف در سطوح سازمانی مختلف ایجاد شود.

ایجاد شبکه‌های اینترنتی امن با پهنای باند مناسب

تجهیز آزمایشگاه‌های تحقیق و توسعه در مراکز تحقیقاتی

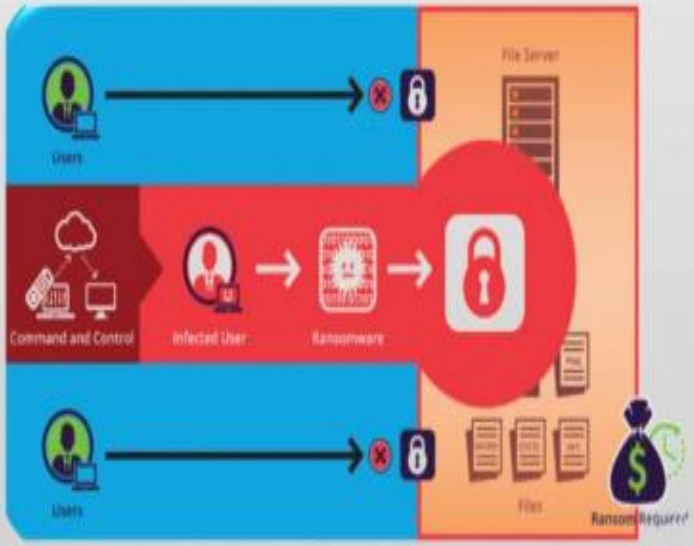
امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- باج افزار نوعی از بد افزارها است که به مجرمان این امکان را می دهد تا بتوانند از طریق یک **کنترل از راه دور**، کامپیوتر قربانی را **قفل** کنند به طوری که کاربر نتواند از سیستم خود استفاده کند و سپس یک پنجره پاپ آپ روی کامپیوتر شخص نمایان کنند تا به او بگویند که **این قفل باز نمی شود تا زمانی که هزینه ای را برای باز کردن آن بپردازید.** [3]

- گاهی هکرها با قرار دادن یک تصویر نامناسب روی کامپیوتر شخص یا اتهام فعالیت غیر قانونی به آن ها، شخص را تحت فشار می گذارند که هر چه سریع تر پول درخواستی آنها را پرداخت کنند تا هکر ها قفل کامپیوتر آنها را باز کنند.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- فرد شیاد یا همان هکر تمام اطلاعات کامپیوتر شما را **رمزگذاری** می کند و هنگامی که کامپیوتر خود را روشن می کنید، با یک پیغام از سوی هکر مواجه شوید که در آن دستورات لازم جهت پرداخت پول به منظور رمزگشایی اطلاعات، توضیح داده شده است. [2]



- معمولا درخواست هکرها این است که وجه مورد نظر با استفاده از **پول دیجیتالی بیت کوین** پرداخت شود؛ زیرا ردیابی فردی که پول از این طریق به او پرداخته می شود؛ غیر ممکن است و هر چقدر در پرداخت وجه درخواست شده تعلل شود، نفوذ باج افزار به سیستم بیشتر می شود.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- به طور کلی باج افزارها چهار نوع می باشند:

1. باج افزار **رمزنگار**
2. باج افزارهای **غیر رمزنگار**
3. باج افزار **موبایلی** (شایع ترین)
4. **Leakware** (تهدید به افشای اطلاعات)

باج افزارهای موبایلی به صورت تصاعدی در حال افزایش هستند و بیشتر سیستم عامل اندروید را هدف قرار داده اند.

این باج افزارها با قرارگیری در گوشی تلفن همراه هوشمند، تمامی اطلاعات آن را رمزنگاری کرده و حتی گوشی قربانی را قفل نمایند. [3]

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

خطرات :

زمانی که شما سهواً خطاهای زیر را انجام دهید، امکان دارد کامپیوتر شما درگیر باج افزار شود: [2]

- باز کردن یک ایمیل حاوی ضمیمه مخرب.
- کلیک روی لینک های مخرب که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارد.
- بازدید از سایت های مخرب که اغلب دارای ماهیت مستهجن هستند.
- باز کردن ماکرو های فاسد در اسناد برنامه.
- اتصال به دستگاه های جانبی usb مثل memory، هارد اکسترنال ، mp3 player و ...
- استفاده از سی دی یا فلاپی های فاسد در کامپیوتر خود.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

جلوگیری از ورود باج افزار:

- هیچ گاه به ایمیل های ناشناس پاسخ ندهید یا ایمیل هایی را که در قسمت spam ایمیلتان قرار دارد را باز نکنید.
- تنها از وب سایت های امن یا وب سایت هایی که می شناسید استفاده کنید.
- قبل از آنلاین شدن، از وجود آنتی ویروس و دیوار آتش مؤثر و به روز رسانی کامپیوتر خود مطمئن شوید و در صورت امکان از antispyware نیز استفاده کنید.
- به طور منظم از اطلاعات خود نسخه پشتیبان تهیه کنید چرا که برخی از باج افزار ها می توانند حتی فایل های مبتنی بر ابر ذخیره سازی را نیز آلوده کنند. [3]

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

اگر درگیر باج افزار شدید :

۱ – برای حذف باج افزار یا دیگر نرم افزارهای مخرب که ممکن است روی کامپیوتر شما نصب شده باشد، یک scan کامل با یک solution امنیتی مناسب و به روز انجام دهید.

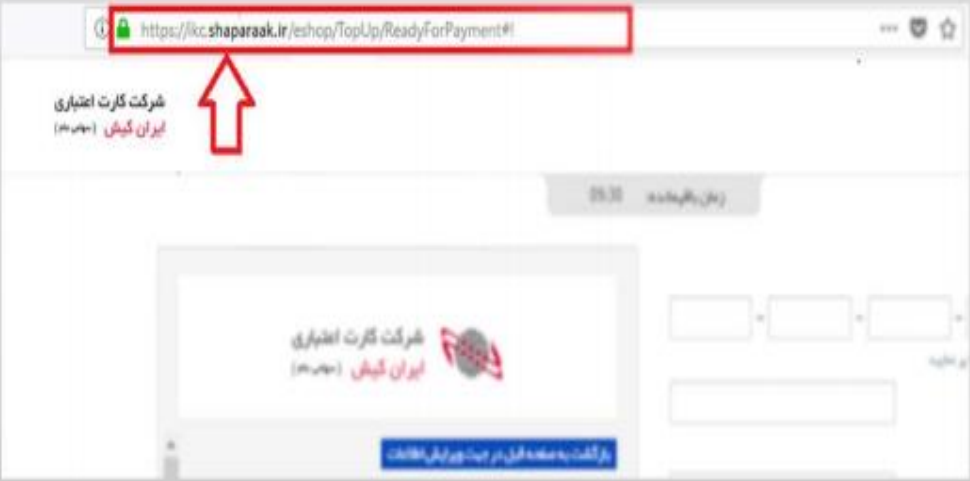
۲ – اگر کامپیوتر شما از طریق باج افزار قفل شده باشد، حتماً برای مشاوره و راهنمایی از یک منبع قابل اعتماد استفاده کنید و به هیچ وجه پول را واریز نکنید چرا که حتی اگر آن ها قفل کامپیوتر شما را باز کنند، پس از مدتی دوباره از شما باج گیری و کامپیوتر شما را قفل می کنند. بنابراین به دنبال یک راه قطعی و مطمئن باشید[2]

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- نوعی تلاش برای بدست آوردن اطلاعات از طریق جعل محسوب می شود.
- **فیشر** (کسی که حمله فیشینگ را انجام می دهد) با استفاده از برخی متدها، اقدام به شبیه سازی یک وبسایت، برنامه و یا حتی یک سرویس نموده و با استفاده از آن، اطلاعات کاربران را به سرقت می برد.[2]

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

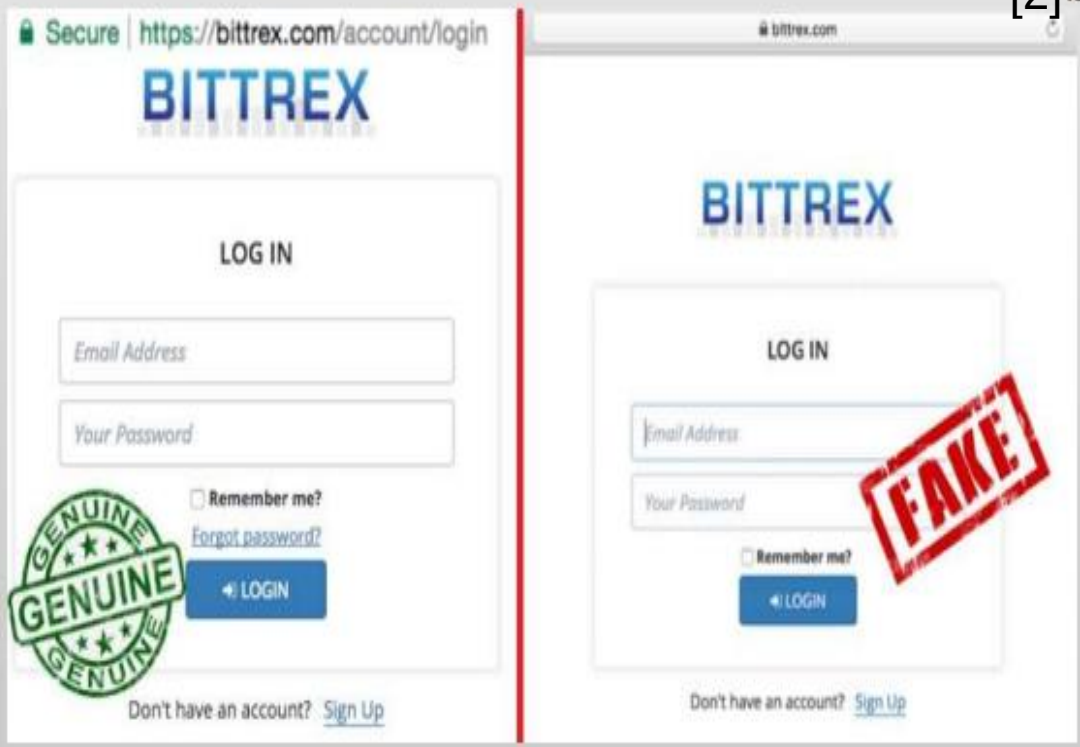
- فیشر اقدام به ساخت یک دامنه با آدرس اینترنتی shaparak.in یا shaparok.ir می نماید و آن را در وب‌سایت‌های مختلف قرار داده و یا از طریق انجام حمله SQL Injection به یک وب سایت هدف، تزریق می‌کند.
- در این هنگام کاربر که قصد خریدی آنلاین را دارد، بجای متصل شدن به درگاه shaparak.ir به درگاه shaparak.in متصل شده و اطلاعات کارت خود از قبیل شماره کارت، رمز دوم، Cvv2و حتی تاریخ انقضای آن را وارد می‌کند.
- نمونه ای از یک آدرس فیشینگ که آدرس به صورت shaparaak و همراه با دو a نوشته شده است.



امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- **جعل وب سایت**

✓ یکی دیگر از حملات فیشینگ شایع، استفاده از **جعل وب سایت** است. در این حمله، فیشر اقدام به ساخت یک صفحه اینترنتی مشابه صفحه اصلی نموده و از طریق اعتمادی که کاربران به آن صفحه اصلی داشته و عدم توجه دقیق به آدرس وب سایت، اقدام به جمع آوری اطلاعات کاربران می نماید.[2]

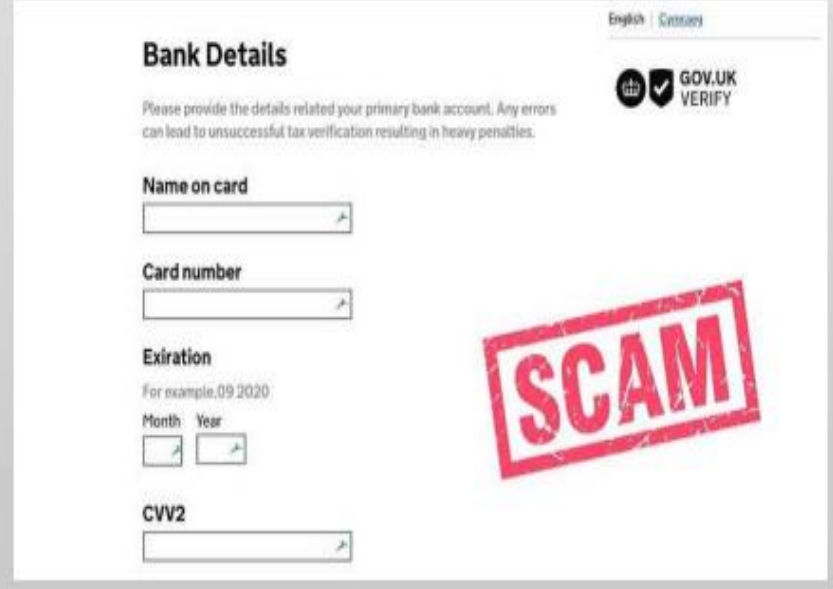


امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- **فیشینگ درگاه های پرداخت**

✓ در این روش فیشر یک وب سایت راه اندازی کرده و در آن اقدام به فروش اقلام و یا سرویس های مختلف می کند. معمولا این وب سایت ها اسم و رسم چندانی نداشته و تنها قیمت پایین خدمات و کالاهای آن ها ترغیب کننده می باشد.

✓ پس از این که کاربر اطلاعات کارت بانکی خود را وارد نمود، بسته به نظر فیشر، یا پیغام خطا در تراکنش و یا پیغام موفقیت آمیز بودن خرید برای کاربر ارسال می گردد ولی اطلاعات کارت بانکی در پایگاه داده وب سایت ذخیره شده و می توان از آن استفاده نمود. [2]



امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

- **فیشینگ تلفنی**

✓ این نوع حمله نیز همچون حمله از طریق ایمیل سعی دارد تا کاربر را مجاب کند تا اطلاعات خود را بازگو نماید.

✓ در این نوع حمله معمولا فیشر با استفاده از یک شماره **تلفن** ناشناس با کاربر تماس گرفته و یا به وی پیام ارسال می کند.

✓ پس از آن فیشر خود را مسئول بانکی که کاربر در آن حساب دارد معرفی کرده و سپس از کاربر می خواهد تا برخی اطلاعات خود را جهت تکمیل پرونده و یا هر موضوع دیگری، بازگو نماید.

✓ اگر کاربر این اطلاعات را به فیشر بدهد، حمله با موفقیت انجام شده است.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

مقابله در برابر حملاتSpear Phishing

در صورتی که ایمیلی از جانب دوست قدیمی یا همکارتان دریافت می‌کنید، از طریق ایمیل پاسخ گوی آن ها نباشید و با آن ها تماس بگیرید. چون ممکن است آدرس درج شده تنها سوء استفاده از اسم اشخاص باشد و در اصل جعلی باشد.

هیچ گاه به شماره تماس‌های موجود در ایمیل ها اعتماد نکنید و سعی کنید شماره های رسمی یک شرکت را پیدا کنید و در خصوص ارسال ایمیل، با آن ها مشورت کنید.

ارسال و دریافت ایمیل ها را کنترل کنید.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

تهدیدهای امنیتی حاصل از بکارگیری شبکه‌های اجتماعی در سازمان‌ها [2]

- ✓ ایمیل‌های فیشینگ که شرحی از سایت‌های شبکه‌های اجتماعی به افراد می‌دهند، اما در واقع آن‌ها را به بازدید از وب‌سایت‌های کلاهبرداری تشویق می‌کنند.
- ✓ پست‌ها و توئیت‌هایی که از طرف همکاران، مشتریان، توزیع کنندگان و سایر افراد است، مشوق افراد در تماس با سایت‌های نامناسب و کلاهبرداری است.
- ✓ کلاهبرداران، سارقان هویت یا هکرها، صفحه و یا حساب افراد را هک می‌کنند و یا اطلاعات محرمانه آنان را به سرقت می‌برند.
- ✓ ممکن است در عکس‌ها یا پیوست‌های پیام، نرم افزارهای جاسوسی وجود داشته باشد.
- ✓ افشای ناخواسته اطلاعات محرمانه توسط افراد (کارمندان، مشتریان یا هر کدام از افرادی که در تماس با سازمان هستند).
- ✓ افشای عمدی اطلاعات محرمانه که به انگیزه‌های متفاوت از قبیل سود مالی، شهرت، کلاهبرداری و در معرض خطر قرار دادن هویت صورت می‌گیرد.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

راهکارهای حفظ امنیت در شبکه‌های اجتماعی [2]

- ✓ دسترسی به حساب کاربری شبکه‌های اجتماعی مورد استفاده شرکت را تنها در اختیار افرادی قرار دهید که برای پیشبرد کار به آن نیاز دارند.
- ✓ آموزش‌های لازم برای استفاده امن از شبکه‌ها
- ✓ دسترسی کسانی که سازمان شما را ترک کردند خیلی فوری متوقف کنید.
- ✓ اگر دسترسی به یکسری از شبکه ها همانند فیس بوک، توئیتر و غیره مورد نیاز است، دسترسی به انواع دیگر شبکه ها را محدود کنید؛ زیرا اگر نظارت کافی نداشته باشید ممکن است آن ها هدف هک کردن قرار بگیرند.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

راهکارهای حفظ امنیت در شبکه‌های اجتماعی [2]

- ✓ در مورد انتشار هرگونه اطلاعات محرمانه در مورد کار، مدیران و کارمندان و یا مشتریان و پروفایلتان در پست ها و توئیت‌ها هشیار باشید.
- ✓ از پسوردهای قوی استفاده کنید.
- ✓ روی ایمیل‌هایی که از طرف رقبای کاری برای شما ارسال می‌شود، نظارت دقیق داشته باشید.
- ✓ به پاسخ‌هایی که به ایمیل‌ها و پست‌های شما داده می شود نظارت داشته باشید.

امنیت سایبری در سازمان ها وامنیت در شبکه های اجتماعی

راهکارهای حفظ امنیت در شبکه‌های اجتماعی [3]

- ✓ یاد بگیرید که چگونه می‌توانید به شکل صحیحی از این شبکه‌ها استفاده کنید.
- ✓ از امکانات موجود در حریم شخصی برای محدود کردن دسترسی دیگران به پروفایلتان استفاده کنید.
- ✓ در مورد افرادی که اجازه استفاده از حساب کاربری شبکه هایتان را به آنها داده‌اید محتاط باشید.
- ✓ مطمئن شوید که شما و همکارانتان در مقابل حملات فیشینگ و دیگر فعالیت‌های مهندسی اجتماعی که با هدف جمع‌آوری پسوردهای رسانه‌های اجتماعی سازمان‌دهی شده است، ایمن هستید و تحت محافظت قرار دارید.
- ✓ مطمئن شوید که نرم افزارهای اینترنتی و فایروال شما به روز و اثربخش هستند و قبل از آنلاین شدن شما اجرا می شوند.
- ✓ نسبت به مدت زمانی که کارمندان و همکاران شما در سایت‌های غیر مرتبط با کار می‌گذرانند آگاه باشید تا بتوانید نظارت بر فعالیت‌های آنلاین آن‌ها داشته باشید.

مصادیق نقض حریم خصوصی در فضای مجازی

- یکی از مهم‌ترین بخش‌های موجود در قانون جرائم رایانه‌ای حوزه مرتبط با نقض حریم خصوصی و انجام فعالیت‌های بزهکارانه در فضای مجازی است. در زیر به مصادیق نقض حریم خصوصی در شبکه‌های اجتماعی که در قانون (علی‌الخصوص قانون جرائم رایانه‌ای) جرم‌انگاری شده است می‌پردازیم[1]:

مصادیق نقض حریم خصوصی در فضای مجازی

- دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا حساب کاربری اشخاص
- شنود غیرمجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم‌افزارهای شنود چت‌های اینترنتی
- دسترسی غیرمجاز به داده‌های سری در حال انتقال در سیستم های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن
- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت

مصادیق نقض حریم خصوصی در فضای مجازی

- نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده
- حذف یا تخریب یا مختل یا غیرقابل‌پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده به‌طور غیرمجاز

مصادیق نقض حریم خصوصی در فضای مجازی

- هتک حیثیت از طریق انتشار یافتن صوت و فیلم تحریف‌شده دیگری به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی
- نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی
- فروش یا انتشار یافتن یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند
- آموزش نحوه ارتکاب جرائم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی

مصادیق نقض حریم خصوصی در فضای مجازی

- از کار انداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز نظیر غیرفعال سازی پایگاه‌داده تارنماها و ممانعت از دسترسی اشخاص به پایگاه‌های اینترنتی شخصی
- ممانعت از دسترسی اشخاص مجاز به داده‌های یا سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز
- ربودن داده‌های متعلق به دیگری به‌طور غیرمجاز

منابع :

۱. محتوای امنیت اطلاعات فناوری مرکز آموزش و پژوهش های توسعه و آینده نگری

۲. کتاب اکفا مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان

۳. کتاب امنیت فناوری اطلاعات

تألیف:

جورج سادوســکای

جیمز اکس. دمپزی

آلــن گرینبرگ

باربارا جی. مک

آلــن شوارتز

ترجمه:

مهدی میردامــادی

زهـــرا شجـــاعی

محمدجواد صمدی