دوره آموزشی:

امنیت کاربری فناوری اطلاعات

مجری:

مرکز آموزش مجتمع فنی مازندران

نشانی : بابل– حدفاصل بین کارگر و کشوری– سرداران۱۰–پلاک۱۳ تلفن: ۱–۳۲۲۵۱۸۰۰

ســـــاری– خیابان معلم– جنب برنامه و بودجه – معلم ۲۹ تلفن: ۱۷–۳۳۲۵۳۳۱۶

E-mail: mfmbabol@yahoo.com **website:** www.mfmbabol.com

مقدمه:

امروزه **امنیت اطلاعات** در سیستم های رایانه ای به عنوان یکی از مسائل مهم دنیای فناوری مطرح است و می‌بایست به مقوله امنیت اطلاعات نه به عنوان یک محصول بلکه به عنوان یک فرآیند نگاه گردد. بدون شک اطلاع رسانی در رابطه با تهدیدات، حملات و نحوه برخورد با آنان، دارای جایگاهی خاص در فرآیند ایمن سازی اطلاعات بوده و لازم است همواره نسبت به آخرین اطلاعات موجود در این زمینه خود را به روز نمائیم. بدین دلیل و با توجه به اهمیت اطلاع رسانی در این زمینه، به اختصار مطالبی در ارتباط با امنیت اطلاعات، هشدارهای امنیتی و ابزارهای برخورد با حملات و تهدیدات امنیتی تقدیم می گردد.

مفهوم سایبر

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر Norbert Wiener در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم ها در سیستم‌های انسانی، ماشینی (و کامپیوتر ها) است.

فضای سایبری

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون (William Gibson) نویسنده داستان علمی تخیلی در کتاب نورومنسر Neuromancer در سال ۱۹۸۴ به کار برده است.

فضای سایبری به مجموعه ای اطلاق میگردد که شامل :زیر ساخت های فناوری اطلاعات، شبکه های ارتباطی آن، سامانه های رایانه ای باشد .این فضا ممکن است به صورت مستقیم به اینترنت متصل باشد و یا تنها در محیط های خاص قابل دسترس باشند .

حمله سایبری

"مگان برنز" در سال ۱۹۹۹ با دیدی کلی تعریف زیر را ارئه می‌دهد «جنگ اطلاعاتی طبقه یا مجموع‌های از تکنیک‌ها شامل جمع آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد آشفتگی و افت کیفیت در اطلاعات است که از طریق آن یکی از دو طرف درگیر بر دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند. به گفته "آرون سود" نایب رئیس مرکز بین المللی سایبری در دانشگاه "جورج میسون" اگر یک هواپیما را ببینید می‌دانید که به نیروی هوایی کشوری تعلق دارد، اما اگر به شما حمله سایبری شود حتی نمی‌توانید بفهمید از کجا به شما حمله شده است!

حملات سایبری دامنه متنوعی دارند، از شوخی‌های معمولی گرفته تا کرم‌های مخرب رایانه‌ای که توسط حافظه‌های قابل حمل جا به جا شده و امنیت کلی کشوری را به مخاطره می‌کشند. از آنجایی که امروزه تمامی زندگی ما به تکنولوژی، رایانه‌ها و اینترنت گره خورده است اطمینان از ایمن بودن این ابزارها بسیار حیاتی است . در چند سال قبل تعداد حملات سایبری به سازمان‌های دولتی، و بویژه هسته‌ای بسیار گسترده شده است. مهم‌ترین حملاتی که در چند سال قبل صورت گرفت، ویروس شعله "فلیم"، ویروس "استاکس‌نت" و "اکتبر سرخ" بوده است که به تازگی رخ داد.

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 .

• سه مشخصه حملات سایبری: ۱-گستردگی ۲- نهفتگی ۳- تنوع

•سرمایه های سایبری :

به تمامی داده ها و اجزای سامانه های سایبری که در یک ساختار وجود دارند سرمایه سایبری اطلاق می شود .

شامل زیرساخت ها و اطلاعات در شبکه های اطلاعاتی و نیز ساختارهای اداری در یک نظام اقتصادی می شود .

آسیب پذیری سایبری :

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

منشاء آسیب پذیریهای سایبری :

ضعف موجود در فناوری مورد استفاده در سامانه سایبری موردنظر، ضعف پیاده سازی (تولید) سامانه سایبری مورد نظر،ضعف تنظیمات و بهره برداری از سامانه سایبری مورد نظر

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

شدت تهدید سایبری :

تهدیدات سایبری علیه سرمایه های ملی سایبری، در پنج سطح طبقه بندی می گردند :خیلی زیاد(فاجعه)، زیاد (بحران)، متوسط (حادثه امنیتی عمده)، کم (حادثه امنیتی) و خیلی کم (رویداد امنیتی)

• دو قسم از تدابیر برای تامین امنیت در فضای سایبری را می توان در نظر گرفت:

۱ .تدابیر مستقیم یا اصلی: این تدابیر به کلیه ی تدابیر فنی و قانونی گفته می شود که برای تامین امنیت دو موضوع زیر به کار می آید:

الف- .داده ها و اطلاعات رایانه ای . ب-سیستم ها و شبکه های رایانه ای و مخابراتی

۲.تدابیر واسطه ای: این تدابیر در پی تنظیم مقررات مناسب برای فضای سایبری است تا به واسطه ی آن هدف اصلی یعنی امنیت فضای واقعی تامین شود .

-جهانی و فرامرزی بودن

- دستیابی آسان به آخرین اطلاعات

- جذابیت

- آزادی اطلاعات و ارتباطات

- چند وجهی و متنوع بودن
-سهولت انجام جرم
- عدم شناسایی آسان مجرمان
- تأثیر گذاری شگرف
-توانایی محدود برای اندازه گیری و ارزیابی وضعیت امنیتی سایبری
- نداشتن معیارهای امنیت سایبری
- دشواری اثبات و اندازه گیری تهدیدات
- رشد تهدیدات با افزایش سیستم های متصل به هم
- ارتباطات طراحی شده نامناسب بین سیستم های کنترلی و شبکه های سامانی
- نبود الزام روشن برای طراحی
-کاهش عملکرد سیستم های قدیمی در صورت ارتقا ایمنی آنها
- افزایش ابزارهای پیچیده ی هکرها
-اشتراک گذاری ناکافی اطلاعات
- هماهنگی ضعیف دولت و صنعت
- درک ضعیف از خطرات سایبری
- سرمایه گذاری کم در امنیت سایبری

حوزه های تهدید :

- تهدیدات فرهنگی جامعه از قبیل رواج بی بندوباری، ایجاد بی اعتقادی، سست کردن باورهای مذهبی، تهاجم فرهنگی
- تهدیدات اجتماعی جامعه از قبیل بسیج و سازماندهی اغتشاشات و ناآرامی های مختلف در کشور و یا تشکیل و هدایت گروه های منحرف
- تهدیدات سیاسی از قبیل انجام اقدامات هماهنگ علیه یک کشور
- تهدیدات اقتصادی و مالی از قبیل اعمال تحریم های اقتصادی از طریق فضای مجازی از قبیل ممانعت از خرید و فروش اینترنتی کالا و خدمات یا جلوگیری از نقل و انتقالات پولی و بانکی
- تهدیدات امنیتی از قبیل تروریسم سایبری

منابع تهدید:

کشورهای خارجی: در سطح جهان موارد متعددی از این دست برای سوء استفاده و تخریب زیرساخت های اطلاعاتی کشورها شامل اینترنت، شبکه های اطلاعاتی، سامانه های رایانه ای و پردازشگرها و کنترل کننده های نهفته در صنایع حیاتی مشاهده شده است .

گروه های خرابکار :به طور روزافزون تهاجمات سایبری این گروه ها که به منظور کسب درآمد به سامانه های سایبری حمله می برند رو به افزایش است .

هکرها: هکرها گاهی اوقات برای اظهار وجود خود وارد شبکه می شوند .

هکرهای سازمان یافته: این افراد معمولاً میزبان های پست الکترونیک را با افزایش بار مواجه نموده و با نفوذ به سایت های شبکه وب پیام های سیاسی خود را اعلام می نمایند.

عوامل ناراضی داخلی: این دسته از عوامل لازم نیست دانش قابل توجهی در خصوص تهاجمات رایانه ای داشته باشند زیرا اطلاع آنها از سیستم مورد هدف غالبًا امکان دسترسی نامحدود برای وارد کردن ضربه به سامانه و یا سرقت اطلاعات سازمان را فراهم می سازد.

تروریست ها :تروریست ها به دنبال تخریب، ناتوان سازی و یا بهره برداری بدخواهانه از زیرساخت های حیاتی به منظور تهدید کردن امنیت ملی، وارد آوردن خسارات سنگین، تضعیف اقتصاد کشور و تخریب روحیه و اعتماد عمومی می باشد.

سازوکارها و روش های تهدید:

انکار خدمات :در این روش دسترسی سامانه به کاربران مجاز و بالعکس از دست می رود. در واقع حمله کننده از یک نقطه شروع به غوطه ور کردن کامپیوترهای هدف در پیام های مختلف و انسداد آمد و شد قانونی داده ها می نماید

انکار توزیع شده خدمات: در این روش به جای شروع حمله از یک منبع، همزمان از تعداد زیادی سامانه توزیع شده اقدام به حمله می کنند. غالباً این کار با استفاده از کرم ها و تکثیر آنها در رایانه های متعدد برای حمله به هدف صورت می گیرد .

ابزارهای سوء استفاده : این ابزار ها در دسترس عموم قرار دارد که می توانند با برخورداری از سطوح مهارتی مختلف آسیب پذیری های موجود در شبکه ها را کشف و از آن طریق وارد شوند.

بمب منطقی : نوعی خرابکاری که در آن برنامه نویس کدی وارد برنامه می کند که در صورت بروز اتفاقی خاص برنامه خود به خود یک فعالیت تخریبی را صورت می دهد.

اسنیفر :برنامه ای است که داده های مسیریابی شده را شنود نموده و با بررسی هر بسته در جریان داده ها به دنبال اطلاعات خاصی مانند کلمه های عبور می گردد.

ارسال هرزنامه : ارسال نامه های پست الکترونیک تجاری ناخواسته که می تواند حاوی سازوکار تحویل نرم افزار های مخرب و سایر تهدیدات سایبری باشد.

سرقت کلمه های عبور و اطلاعات مالی: با استفاده از هرزنامه افراد را فریب می دهد تا اطلاعات حساس خود را افشا نمایند .

ساخت وب سایت جعلی: ایجاد یک وب سایت فریب برای تقلید از یک سایت واقعی و مشروع .

فریب: روشی که دزدان کلمه عبور برای فریب کاربران و متقاعد کردن آنها از ارتباط با وب سایت معتبر بکار می برند .

بات نت : بات ها معمولاً به صورت مخفیانه در سامانه هدف نصب می شوند و امکان کنترل از راه دور رایانه مورد هدف را به کاربر غیر مجاز می دهند تا اهداف خرابکارانه خود را محقق کنند.

انواع نفوذ گران و بازیگران تهدید :

گروه نفوذگران کلاه سفید :هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه ای انجام ندهد را یک هکر کلاه سفید می خوانند که در حقیقت متخصصین شبکه ای هستند که چاله های امنیتی شبکه را پیدا کرده و به مسئولان گزارش می دهند.

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 می پردازند.

گروه نفوذگران کلاه خاکستری : اشخاصی هستند که حد وسط دو تعریف کلاه سفید و سیاه می باشند.

گروه نفوذگران کلاه صورتی :این افراد آدم های کم سوادی هستند که با چند نرم افزار خرابکارانه به آزار و اذیت بقیه اقدام می کنند .

انگیزه های تهدید: •تجاری •مالی •تلافی جویانه •تفننی

• Computer Emergency Response Team (CERT)

اهداف CERT عبارتند از:

• ایجاد چارچوبی برای ساخت قابلیت اطمینان و پاسخ مناسب به حوادث

• محافظت از سرمایه های حساس اطلاعاتی

• پاسخ مناسب به ریسک های در حال تغییر به طور مداوم

• تمرکز مدیریت تداوم کسب و کار به تعریف تأثیر بالقوه تهدیدات متوجه تداوم فعالیت های کسب و کار

•ایجاد آمادگی برای پاسخ به حادثه قبل از آنکه منجر به توقف سرویس گردد

• ایجاد ساختار پاسخ و بازیابی از حوادث و خرابی ها

•ایجاد اطمینان از تداوم فعالیت های حیاتی کسب و کار که توسط خدمات فناوری اطلاعات پشتیبانی می شوند .

مهندسی اجتماعی و راه های مقابله با آن

مهندسی اجتماعی (Social engineering) به معنی عملی است که از طریق فریب افراد با انجام اقدامات خاص، منجر به افشای اطلاعات شخصی، مالی و ... می شود یا به تعبیری دیگر شیوه و ترفندی فریبکارانه برای جلب اطمینان افراد، برای دریافت اطلاعات از آن ها می باشد.

مهندسی اجتماعی (Social engineering) به معنی عملی است که از طریق فریب افراد با انجام اقدامات خاص، منجر به افشای اطلاعات شخصی، مالی و ... می شود یا به تعبیری دیگر شیوه و ترفندی فریبکارانه برای جلب اطمینان افراد، برای دریافت اطلاعات از آن ها می باشد.

شیوه ها و ترفند ها

–بسیاری از حملات مهندسی اجتماعی، نیازی به اطلاعات فنی و تخصصی ندارند و لازم نیست تا یک متخصص رایانه و یا یک هکر حرفه ای به شما حمله کند . باید نسبت به محیط اطراف آگاه بود چرا که هر یک از افراد جامعه می توانند، نقش یک مهاجم را ایفا کنند.

–در اکثر حملات مهندسی اجتماعی، پیشنهاداتی به شما ارائه می شود که در نگاه اول، بسیار پر سود و جذاب به نظر می رسد باید تلاش کرد تا تا بر وسوسه پاسخگویی به این دسته از پیشنهادات غلبه کرد چرا که برخی از آن ها، طعمه هایی برای حملات مهندسی اجتماعی هستند.

–مهندسین اجتماعی می توانند اطلاعات را به شیوه های مختلفی از قربانیان خود به دست آورند آنها غالبا ماهرانه صحبت می کنند و بر روی پیشرفت مکالمات خود تمرکز می کنند به نحوی که وقت زیادی به قربانیان خود نمی دهند تا در مورد آن چه که می گویند فکر کنند.

–حملات مهندسی اجتماعی شما را در حالت هایی نظیر اضطراب، هیجان، ترس و به طور کلی حالات خاص روانی قرار می دهد تا تمرکز و توان تصمیمی گیری شما را کاهش دهد. لذا باید از تصمیم گیری های شتاب زده پرهیز کنید.

روش های تهاجم مهندسین اجتماعی

–طعمه گذاری مهندسین اجتماعی معمولا با ابزار های فیزیکی انجام می شود و مهاجم وسایلی نظیر لوح فشرده یا فلش دیسک که حاوی بدافزار هستند را به عناوین مختلفی نظیر هدایای تبلیغاتی و مطالب مفید و جذاب در اختیار قربانیان قرار می دهد که در نهایت با استفاده قربانی از این وسایل و فعال کردن بدافزار در سیستم شخصی خود، باعث می شود که مسیر دسترسی مهاجم به اطلاعات شخصی او فراهم شود.

–در نوع دیگری از حملات، ابتدا مهاجم طعمه خود را که معمولا پیامی جعلی با ظاهری مشابه پیام های یک نهاد معتبر (نظیر بانک) است را برای تعداد زیادی از کاربران ارسال می کند و سپس منتظر می ماند به این امید که افراد هدف حمله، فریب خورده و خود را در دام وی گرفتار نمایند. حال ممکن است این کار با کلیک بر روی یک پیوند باشد یا ارسال مشخصات فردی.

–یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد . مثلا در یک سازمان یا شرکت وانمود کند که کارمند جدید است، یک تعمیرکار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تعیین هویت خود به شما ارایه دهد. یک مهاجم با طرح سوالات متعدد و برقراری یک ارتباط منطقی بین آن ها می تواند به بخش هایی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه سازمان شما، دستیابی پیدا نماید.

چگونگی مصون ماندن از حملات مهندسین اجتماعی

–ساده ترین و کارآمد ترین راه برای مقابله با حملات مهندسی اجتماعی، آموزش افراد و افزایش آگاهی آنهاست. اگر تک تک افراد، آگاهی کافی نسبت به محیط خود داشته باشند، در لحظات حساس، به درستی و بر اساس اصول، تصمیمی گیری می کنند که در این صورت هیچ حمله مهندسی اجتماعی موفقی، رخ نخواهد داد.

–مهمترین منبع اطلاعاتی مهاجمان در حملات مهندسی اجتماعی، مطالبی است که در مورد افراد در منابعی نظیر اینترنت قرار دارد و به سادگی قابل دسترس است به ویژه اطلاعاتی که خود فرد در شبکه های اجتماعی منتشر می کند . در صورتی که افراد با مطالب شخصی خود آگاهانه رفتار کرده و آن ها را در معرض دید عموم قرار ندهند، امکان استفاده از این اطلاعات در حملات مهندسی اجتماعی نیز کاهش خواهد یافت.

–رسانه های اجتماعی، خود نیز یکی از مشکلات عمده بحساب می آیند. شما باید دسترسی به شبکه های اجتماعی خود را ایمن سازید و همواره مراقب باشید که در حال برقراری ارتباط با چه کسی می باشید. شبکه های اجتماعی همواره، منبع اطلاعاتی خوبی برای حملات مبتنی بر مهندسی اجتماعی به شمار می آیند چرا که پر است از اطلاعات شخصی حقیقی.

–همیشه و در همه جا حتی در مکان های عمومی چون داخل تاکسی یا مترو در حال تعامل با دیگران، مراقب واکشی اطلاعات و تخلیه اطلاعاتی از سوی دیگران باشید هیچگاه اطلاعات اضافی در اختیار سایر افراد قرار ندهید و توجه داشته باشید که هر مکالمه به ظاهر بی ضرر می تواند در واقع اطلاعات ارزشمندی را برای مهاجمان با تجربه، به همراه داشته باشد.

اقدامات لازم در صورت بروز تهاجم

–در صورتی که فکر می کنید به هر دلیلی اطلاعات حساس سازمان خود را در اختیار دیگران (افراد غیرمجاز) قرار داده اید، بلافاصله موضوع را به قید فوریت به رئیس حراست و مسئول حفاظت فناوری اطلاعات یا سایر مسئولین مربوطه اطلاع دهید. آنان می توانند در خصوص هر گونه فعالیت های غیرمعمول و یا مشکوک، هشدارهای لازم را در اسرع وقت در اختیار دیگران قرار دهند.

–در صورتی که فکر می کنید اطلاعات مالی شما ممکن است در معرض تهدید قرار گرفته شده باشد بلافاصله با موسسه مالی خود تماس حاصل نموده و تمامی حساب های مالی در معرض تهدید را مسدود نمائید.

–گزارشی در خصوص نوع تهاجم تهیه نموده و آن را در اختیار سازمان های ذیربط قانونی قرار دهید.

امنیت در شبکه‌های اجتماعی

شبکه‌های اجتماعی، گونه‌ای از وب‌سایت‌های اینترنتی هستند که افراد، گروه‌ها و سازمان‌ها، در آن‌ها پیرامون یک یا چند ویژگی مشترک گردهم می‌آیند و اطّلاعات، مطالب و محتواهای خود را با یکدیگر به اشتراک می‌گذارند. با ظهور و بروز تکنولوژی‌های جدید وب مثل وب ۲.۰ و وب معنایی، شبکه‌های اجتماعی که مبتنی بر تعامل کاربران در ارتباط‌گیری، تولید و به اشتراک‌گذاری محتوا هستند، به وجود آمدند تا جایی که مجموع کاربران معروف‌ترین شبکه‌های اجتماعی اینترنت، به بیشتر از یک میلیارد کاربر رسیده‌است.

کارکردهای شبکه‌های اجتماعی

در هر کشور و هر جامعه‌ای متناسب با فرهنگ، تعاملات اجتماعی و فعّالیّت‌های سیاسی و اقتصادی، کارکردهای شبکه‌های اجتماعی با هم متفاوت است. امّا برخی کارکردهای شبکه‌ای در تمامی جوامع با هم مشترک است. مهم‌ترین کارکرد شبکه‌های اجتماعی ایجاد گروه‌ها و دسته‌های ارتباطی (Community) پیرامون ویژگی یا ویژگی‌های خاص است. همچنین کارکردهای اقتصادی، مبتنی بر بازاریابی اجتماعی نیز از دیگر کارکردهای این شبکه‌هاست. کارکرد دیگری که برای این شبکه‌ها متصوّر است کارکرد سیاسی است. ایجاد کمپین‌های سیاسی، فعّالیّت‌های دسته‌ها، گروه‌ها و افراد سیاسی در یک فضای اجتماعی اینترنتی از کارکردهای شبکه‌های اجتماعی است.

البته کارکرد سیاسی این شبکه‌ها مورد سوء استفاده‌ی قدرت‌های استکباری قرار گرفته‌است. به نحوی که با طرّاحی اقدامات تبلیغاتی و رسانه‌ای، از وب‌سایت شبکه‌های اجتماعی به عنوان ابزاری برای ایجاد آشوب و بلوا، جنگ روانی و دخالت در امور مختلف کشورهای آزاد استفاده می‌کنند. اقدامات خصمانه‌ی امریکا و سرویس‌های جاسوسی و اطّلاعاتی سیا و موساد در سال‌های اخیر در فضای شبکه‌های اجتماعی که ایرانی‌ها از آن استفاده می‌کنند، از این دست محسوب می‌شود.

شبکه‌های اجتماعی و حریم خصوصی

حریم خصوصی و محرمانگی اطّلاعات شخصی، یکی از مهم‌ترین و جنجالی‌ترین مباحثی است که از ابتدای همگانی شدن اینترنت و بعدتر با ظهور و بروز شبکه‌های اجتماعی وجود داشته‌است. تقریباً هیچ کسی پیدا نمی‌شود که بخواهد اطّلاعات شخصیِ فردی و خانوادگی خود را به راحتی در اختیار دیگران بگذارد.

در کشورهای غربی، سیاست محرمانگی (Privacy Policy) یکی از ارکان کاربری اینترنت است، به نحوی که قوانین و مقرّرات موضوعه ایجاب می‌کند که در تعامل بین وب‌سایت‌ها، خدمات‌دهندگان اینترنتی و کاربران، ضمن تعریف سیاست محرمانگی، این امر به نحو مطلوبی در وب‌سایت خدمات‌دهنده به رؤیت کاربر رسیده، حقوق و تکالیف وی یادآوری گردد. بر اساس سیاست محرمانگی خدمات‌دهندگان و کاربران توافق می‌کنند که چه اطّلاعاتی از آنان به نمایش درآید یا به هر نحو مورد استفاده قرار گیرد. اگر به هر شکل دیگری، خارج از توافق‌نامه‌ی محرمانگی، اطّلاعات کاربران مورد سوءاستفاده قرار گیرد، کاربران امکان اقامه‌ی دعوی و طرح شکایت را علیه وب‌سایت خدمات‌دهنده خواهند داشت. معمولاً در شبکه‌های اجتماعی، جزئی‌ترین اطّلاعات کاربران نیز قابل دریافت و انتشار است. علاقمندی‌ها، میزان تحصیلات، ارتباطات خانوادگی، ارتباطات دوستانه، شغل، محلّ زندگی، محل تحصیل و محلّ تولّد و بسیاری از جزئیات دیگر مورد سوال قرار می‌گیرد. برخی از وب‌سایت‌های شبکه‌های اجتماعی، حتّی رنگ مو، رنگ چشم و اندازه‌ی قدّ کاربر را نیز می‌پرسند.

شبکه‌های اجتماعی و کاربران ایرانی

اگرچه برخی از شبکه‌های اجتماعی خارجی با توجّه به قوانین و مقرّرات جمهوری اسلامی ایران و فعّالیّت‌های مجرمانه‌ای که در فضای آن سایت‌ها صورت می‌گیرد، خارج از دسترسی عادّی قرار دارند، لکن به هر حال بخشی از کاربران ایرانی در این شبکه‌ها عضویت داشته و به انحاء مختلف به آن‌ها دسترسی دارند.

متأسفانه، بررسی‌ها نشان می‌دهد که حضور بسیاری از کاربران ایرانی در فضای شبکه‌های اجتماعی، با مخاطراتی در رابطه با تهدید حریم خصوصی آنان مواجه است و سهل‌انگاری این دسته از کاربران، گاه صدمات و لطمات جدّی بر آنان وارد کرده‌است.

بایستی این حقیقت را پذیرفت که مهم‌ترین چالش شبکه‌های اجتماعی اینترنتی، موضوع «اعتماد» به مخاطب یا کسانی است که در لیست دوستان شما قرار می‌گیرند. مطالعه‌ی سبک کاربری کاربران ایرانی نشان می‌دهد که معمولاً کاربران درخواست سایر کاربران برای دوستی را به راحتی می‌پذیرند. این در حالی است که به طور معمول، در شبکه‌های اجتماعی دوست‌یابی صورت نمی‌پذیرد و تنها دوستان و آشنایان در فضای واقعی در این فضا نیز نسبت به اتّصال و اشتراک‌گذاری اطّلاعات و محتوا اقدام می‌کنند. در زیر به برخی از نکات مهم در رابطه با تامین امنیت در فضای شبکه‌های اجتماعی اشاره می‌شود.

۱ .مراقب جعل هویت باشید: یکی از مهم‌ترین موضوعاتی که کاربران را تهدید می‌کند موضوع جعل هویت است. بخصوص در زمانی که کاربر در زمینه‌ای جزو افراد سرشناس و شناخته‌شده باشد. در صورتی که در حیطه‌ی کسب و کار یا حوزه‌ی اجتماعی خود، فرد سرشناسی هستید، ممکن است افراد دیگری با سوءاستفاده از محتواها و اطّلاعاتی که شما

به صورت عمومی به اشتراک گذاشته‌اید، با نام و هویّت جعلی شما و با راه‌اندازی صفحات مشابه دست به اخّاذی، کلاهبرداری و سایر اقدامات مجرمانه بزنند. از این رو هوشیاری در حفظ اطّلاعات و محتواهای خصوصی کاملاً اهمیّت دارد. همچنین در صورتی که متوجّه شدید شخصی با هویّت شما اقدامات مجرمانه صورت می‌دهد، موضوع را به پلیس فتا اعلام کنید.

۲ .اسرار ملّی و سازمانی را افشاء نکنید: سازمان، شرکت یا موسّسه‌ای که در آن کار می‌کنید، قطعاً اطّلاعاتی را در اختیار شما می‌گذارد که انتظار دارد شما آن‌ها را به صورت محرمانه نزد خود نگه‌دارید. برخی از شبکه‌های اجتماعی نیز طوری طرّاحی گردیده‌اند که ناخواسته افراد را به ورطه‌ی جاسوسی می‌کشانند. برای مثال برخی شبکه‌های اجتماعی مبتنی بر جانمایی که افراد نام و نشان خیابان‌ها، اماکن و مراکز مهم و حسّاس را به اشتراک می‌گذارند، عملاً کارکرد جاسوسی دارند و به راحتی این امکان را به دشمن می‌دهند که به اطّلاعات مکانی مراکز مهم، حسّاس و حیاتی بدون کمترین زحمتی دسترسی داشته باشد.

۳ .مراقب کرم‌های رایانه‌ای و تروجان‌ها باشید: برخی از خدمات شبکه‌های اجتماعی مثل اپلیکیشن‌ها در دل خود، کرم‌های رایانه‌ای و تروجان‌ها را انتشار می‌دهند. بنابر این در فضای شبکه‌های اجتماعی، به هر خدمتی که از سوی کاربران دیگر به شما پیشنهاد می‌شود اعتماد نکنید.

۴ .توافق‌نامه‌ی محرمانگی اطّلاعات را مطالعه کنید: با مطالعه‌ی توافق‌نامه‌ی سیاست‌های محرمانگی، متوجّه خواهید شد که کدام دسته از اطّلاعات که شما در شبکه‌های اجتماعی به اشتراک می‌گذارید ممکن است در معرض خطر قرار گیرد. این کار به شما کمک کنید با دقّت بیشتری از این شبکه‌ها استفاده کنید.

۵ .به هر ناشناسی اعتماد نکنید: فضای شبکه‌های اجتماعی مملو از کاربرانی است که با هویّت‌های جعلی و برای مقاصد خاص مثل کلاهبرداری، اشاعه‌ی فحشاء و سایر اقدامات غیرقانونی و مجرمانه نسبت به ارتباط‌گیری با کاربران اقدام می‌کنند. از این رو از پذیرفتن افرادی که با هویّت، تصاویر و طرح مطالب اغواکننده سعی در ارتباط‌گیری و افزودن شما به لیست دوستان یا علاقمندان صفحه‌ی خود را دارند، اجتناب کنید.

۶ .تنظیمات حریم خصوصی را انجام دهید: تمامی شبکه‌های اجتماعی، ابزارهایی را در اختیار شما می‌گذارند که نسبت به تنظیم حوزه‌ی حریم خصوصی خود اقدام کنید. با استفاده از این ابزارها می‌توانید با خیال راحت‌تر نسبت به اشتراک‌گذاری اطّلاعات با دوستان اقدام کنید و دسترسی دیگران را محدود نمایید.

بهداشت سایبری

امنیت سیستم:

-هر سیستم عامل و برنامه کاربری در معرض خطر نقص های امنیتی است
- عرضه کنندگان نرم افزار برای رفع نقص های امنیتی وصله ارائه می کنند.
-با نصب به موقع وصله های امنیتی می توان از تسخیر سیستم جلوگیری کرد.
-کاربران باید وصله های امنیتی را نصب نموده و نرم افزار را پیکربندی نمایند

امنیت سایبری

امنیت سایبری رابط، یکپارچه سازی است و گاهی اوقات با سایر حوزه ها همپوشانی دارد، این خطوط مبهم می توانند توجه امنیتی را به خطر بیاندازند.این قضیه می تواند عواقب فاجعه بار داشته باشد و می تواند کسب و کار شما را در معرض خطر قرار دهد.

امنیت سایبری همانند حفاظت از داده ها نیست بلکه بیشتر مربوط به حریم خصوصی و نحوه استفاده از داده ها است هرچند که حفظ حریم خصوصی و امنیت آسان است. قرار دادن میله های آهن در یک پنجره، امنیت بیشتری را به وجود می آورد، اما برای حفظ حریم خصوصی هیچ کاری نمی کند، در حالی که قرار دادن یک پرده اثر معکوس دارد. امنیت سایبری همانند پشتیبان گیری داده ها نیست، که تحت دامنه تداوم کسب و کار قرار می گیرد. داشتن یک برنامه پشتیبان گیری و بازیابی خوب در محل، پس از هر سناریویی حیاتی است چرا که منجر به از دست رفتن اطلاعات یا سازش می شود.

امنیت سایبری به بیان دیگر

ساده ترین تعریف cyber security از طریق مقایسه و مخالفت با امنیت اطلاعات است: در حالی که امنیت اطلاعات محافظت از اطلاعات شما را از هر گونه دسترسی غیر مجاز، امنیت سایبری آن را از دسترسی آنلاین غیر مجاز محافظت می کند. این تعریف ساده بود، اما برای یک جایگزین رسمی و جامع تر:

"***امنیت سایبری*** مجموعه ابزارها، سیاست ها، مفاهیم امنیتی، امنیت، دستورالعمل ها رویکردهای مدیریت ریسک اقدامات، آموزش، بهترین شیوه ها، اطمینان و فن آوری هایی که می تواند برای محافظت از محیط زیست سایبری و سازمان ها و دارایی های کاربر استفاده شود" .

امنیت سایبری یک فرآیند است

بهتر است فکر نکنید که cyber security یک راه حل، فن آوری و چیزی بیشتر نیست. بله، شامل ابزار و فن آوری هایی است که در مبارزه روزمره برای حفظ انطباق و یکپارچگی اطلاعات استفاده می شود؛ اما امنیت سایبر فرآیند کسب و کار است. این بدان معنی است که توجه مدیران به سطح مورد نیاز و درک آن است که مانند هر فرایند تجاری دیگر می تواند با نیازهای کسب و کار و واکنش به تغییرات در تهدید، سازگار شود. قابلیت های cyber security سازمانی باید نه تنها با اشتیاق شما برای ریسک، بلکه با اهداف استراتژیک گسترده تر کسب و کار هماهنگ شود.

راه های ایجاد امنیت در سیستم های خانگی و اداری :

-نصب نسخه اصلی آنتی ویروس و نرم افزار ضد جاسوسی

- به روز رسانی مستمر نرم افزار ها

- ذخیره سازی فایل های مهم و حساس در رسانه های قابل حمل مثل کول دیسک ها و سی دی و ...

- امنیت رمز عبور

- رمز نگاری پیشرفته پوشه ها و فایل ها

راه های ایجاد امنیت در سیستم های 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

بد افزار

برای بسیاری از ما پیش آمده‌است که در هنگام کار با کامپیوتر متوجه شویم که سیستم به درستی عمل نمی‌کند و یا دائم ما را به انجام کار تکراری مجبور می‌کند. در این حالت است که متوجه می‌شویم که سیستم ما به ویروس آلوده

شده‌است Malware .یا بدافزار در اصل قطعه کدهایی هستند که توسط برنامه نویسان نوشته میشوند تا بوسیله آن بدون اجازه مالک سیستم، آن را آلوده و اقدام به کارهای ناخواسته یا خرابکارانه کنند. این واژه به صورت عمومی به تمامی کدها و برنامه های مخرب اطلاق میشود و به طور کلی هر نوع کدی که روی سیستم شما قرار بگیرد و عملیاتی ناخواسته را انجام دهد به عنوان بدافزار شناخته میشود Malware .میتواند گوشی تلفن، تبلت و کامپیوترها را آلوده کند . بد افزارپس از ورود به سیستم شما میتواند کارهایی مانند ارسال ایمیل های اسپم، سرقت اطلاعات و رمز عبور های اکانت هاستینگ و ... انجام دهد.

بدافزارها میتوانند از انواع روش ها و تکنیک های مختلف برای اجرای خود استفاده کنند . مثلا بعضی از آنها از سیستم شما به عنوان قربانی برای انجام عملیات تخریب روی دیگر سیستم ها استفاده میکنند، بعضی از آنها اقدام به جمع آوری اطلاعات شخصی کاربران مانند شماره حساب بانکی، رمز عبور و نام های کاربری و ... میکنند و حتی ممکن است باعث تخریب در سیستم کاربران شوند.

Malwareهمچنین می‌تواند از طریق حفره های امنیتی موجود بر روی برنامه سایت شما وارد سیستم شود.

انواع بدافزارها میتواند شامل موارد زیر باشد:

- virus ویروس ها: برنامه ای که با کپی کردن برنامه های دیگر ، سکتورهای بوت سیستم با داکیومنت ها تکثیر شده و فایل های کامپیوترو نیز اپلیکیشن هارا تغییر می دهد یا به آنها آسیب می رساند

-Wormکرم ها : یک ویروس خود تکثیر که فایل ها را تغییر نمی دهند اما در حافظه کامپیوتر مستقر شده و خود را تکثیر می نماید

Backdoor بکدر: یک شیوه غیر مجاز برای دسترسی به سیستم و دورزدن مکانیزم های امنیتی آن

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

Trojan تروجن: برنامه ای که مجاز به نظر میرسد اما پس از اجرا اقدامات مخرب انجام می دهد

Logic Bomb : برنامه ای که یک ویروس با کرم را منتشر می کند

جاسوس افزار Spyware: جاسوس افزارها شامل تروجان ها و سایر نرم افزارهای مخرب هستند که بدون اطلاع کاربر اطلاعات شخصی وی را از سیستم سرقت می نمایند. مانند: کی لاگر Keylogger

کی لاگر Keylogger : کی لاگر یک دستگاه سخت افزاری یا یک برنامه نرم افزاری کوچک است که هر کلیدی را که بر روی صفحه کلید کاربر فشرده می شود ثبت می کند .

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

۱- مهندسی اجتماعی: فریب دادن افراد برای فاش کردن پسورد یا سایر اطلاعاتی که به حدس پسورد کمک می کنند

۲- مخفیانه نگاه کردن: مخفیانه نگاه کردن به کسی که در حال وارد نمودن پسورد است

۳- حمله دیکشنری: لیستی از کلمات از پیش تعریف شده برای یافتن پسورد استفاده می کند

۴- بروت فورس: تلاش برای ترکیب کاراکترهای مختلف تا زمانی که پسورد صحیح پیدا شود.

۵- حدس زدن: تست کردن پسوردهای مختلف تا زمانی که یکی از آن ها درست باشد

پخش بدافزار:

- **از طریق سایت های آلوده:** بازدید از سایت های آلوده ممکن است منجر به نصب نرم افزارهای مخرب (که به منظور سرقت اطلاعات طراحی شده اند) بر روی کامپیوتر کاربر شود.
- **از طریق کارت حافظه های USB** : ویروس یک فایل autorun.inf ایجاد می کند که یک فایل فقط خواندنی و پنهان است. زمانی کاربر فایل های درون USBرا باز می کند autorun. Inf اجرا شده و فایل های وردپرس را در سیستم کپی می کند.
- **از طریق پیوست های ایمیل:** ایمیل های دارای پیوست ممکن است حاوی بد افزار باشند . با کلیک بر روی پیوست یک برنامه مخرب بر روی کامپیوتر نصب می گردد.
- **از طریق پوشه های اشتراک گذاری شده:** بد افزار ممکن است از طریق اشتراک گذاری های شبکه پخش شود بدافزار ممکن است از طریق بدافزار ممکن است با کپی نمودن خود در پوشه های به اشتراک گذاشته شده گسترش یابد
- **از طریق کدک:** اگر کاربری بخواهد یک پلیر برای تماشای ویدئو دانلود و نصب نماید، کدک ممکن سیستم دانلود می شود.

- **از طریق دانلودها:** دانلود نرم افزار، آهنگ، عکس و ویدئو از سایت های نامعتبر ممکن است منجربه دانلود یک فایل مخرب آلوده به ویروس، کرم، تروجان و غیره گردد .اپلیکیشن های مخرب زیادی در اینترنت وجود دارند که با جلات تحریک کننده می توانند 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 ویروس هایی را نشان می دهد که وجود ندارند .با کلیک بر روی دکمه Register یا Scanبدافزار بر روی سیستم دانلود می شود.

نشانه های وجود یک بدافزار در رایانه:

- پاپ آپ ها

-از کار افتادن ناگهانی سیستم

- فعالیت مشکوک هارد دیسک

-کمبود فضا روی هارد دیسک

- فعالیت غیرطبیعی شبکه

- تعویض صفحه نخست مرورگر، باز شدن سایت ها به صورت ناخواسته

-پیغام های غیرطبیعی یا باز شدن ناخواسته نرم افزارها

- کار نکردن نرم افزارهای امنیتی

-دریافت پیغام های غیرعادی توسط دوستانتان

اشتراک گذاری فایل peer-to-peer :

-امکان به اشتراک گذاری موسیقی، تصاویر، داکیومنت ها و برنامه های نرم افزاری بین دو کامپیوتر را از طریق بستر اینترنت فراهم می آورد .

- فایل های به اشتراک گذاشته شده ممکن است حاوی خطرات امنیتی مانند ویروس، جاسوس افزار و سایر نرم افزارهای مخرب باشند .

- مهاجمان می توانند بدافزار را به عنوان یک اپلیکیشن مفید جلوه دهند.

دستورالعمل های ابزارهای امنیتی ویندوز:

- قفل نمودن سیستم زمانی که از آن استفاده نمی شود

- ایجاد پسورد قوی

- غیرفعال نمودن حساب کاربریGuest

- قفل نمودن اکانت بعد از چندین بار ورود ناموفق

- تغییر نام حساب کاربریAdministrator

-غیر فعال نمودن Start up

- اعمال وصله های امنیتی نرم افزارها

-استفاده فایروال ویندوز

-استفاده از NTFS

- استفاده از رمزگذاری فایل سیستم ویندوز

-فعال نمودن Bitlocker

- غیر فعال نمودن سرویس های غیر ضروری

-متوقف نمودن پردازش های غیر ضروری

- پیگربندی سیاست های ممیزی

- مخفی نمودن فایل ها و پوشه ها

- غیر فعال نمودن اشتراک گذاری فایل

- مخفی نمودن فایل ها و پوشه ها

-غیر فعال نمودن اشتراک گذاری فایل

- استفاده از کنترل حساب کاربری ویندوز

- پیاده سازی مکانیزم های پیشگیری از بدافزار

قفل نمودن سیستم زمانی که از آن استفاده نمی شود : در ویندوز ۱۰ به ۲ طریق می توان سیستم را قفل نمود:

الف- راست کلیک بر روی صفحه Desktop و انتخاب گزینه Personalize

ب- فشردن همزمان + Windows

توصیه هایی در رابطه با به روزرسانی:

-همیشه سیستم عامل و برنامه های را با آخرین وصله های امنیتی وصله نمایید .

-وصله های امنیتی را فقط از منابع معتبر دانلود کنید، ترجیحا از سایت های معتبر عرضه کننده ی نرم افزار مانند مایکروسافت .

-تنظیمات را به گونه ای تنظیم نمایید که هشدار عرضه کنندگان در رابطه با آسیب پذیری ها برای شما ارسال شود .

-فایل های اجرایی را که از منابع مشکوک هستند باز نکنید .

-وصله های امنیتی را از طریق ایمیل ارسال نکنید.

-برای نصب آسانتر به روز رسانی ها از ابزارهای مدیریت پچ استفاده نمایید.

اعمال وصله های امنیتی نرم افزارها:

-به روز رسانی های نرم افزار برای به روز نگه داشتن سیستم عامل و سایر نرم افزارها مورد استفاده قرار می گیرد.

- به روز رسانی ها باید از سایت عرضه کنندگان نرم افزار نصب گردد

- به روزرسانی خودکار می تواند به صورت زمان بندی شده باشد.

- به روزرسانی ها می تواند به صورت دستی یا خودکار انجام گیرد.

- بعد از شروع به روز رسانی نیازی به دخالت کاربر وجود ندارد

امنیت رمز عبور:

-طول رمزهای عبور خود را بیشتر از ۸ کاراکتر (حرف) انتخاب کنید

-درون رمز عبور خود، هم از حروف بزرگ و هم از حروف کوچک استفاده کنید .

-درون رمز عبور خود، از اعداد نیز استفاده کنید .

-درون رمز عبور خود، از علائم انگلیسی مانند نقطه، فاصله، اعشار، و علائم دیگر مانند «...,?,,*,,_,=,+,/,\,|,~,!,@,#,$,%,^,&استفاده کنید.

-درون رمز عبور خود، از حروف اضافه انگلیسی «,,.,:,;,'," و ...» استفاده کند

-درون رمز عبور خود، از انواع پرانتز ({,},(,),[,]) استفاده کنید

سیستم های مختلف ایمیل چگونه کار می کنند؟

-ایمیل یک روش تبادل پیام های دیجیتالی از یک فرستنده به یک یا چند گیرنده است .

- شرکت هایی مانند Microsoft ، Yahoo، Google، AOLاز حساب های ایمیل رایگان خود استفاده می کنند .

- حساب های ایمیل، از هر مرورگر وب یا کلاینت ایمیل مانند Outlook Microsoft ، Thunderbird Mozillaو غیره قابل دسترسی است

امنیت ایمیل:

- ارتباط از طریق ایمیل به طور ۱۰۰ درصد امن نیست

-. ایمیل های ناامن، به مهاجمان اجازه می دهند تا به اطلاعات شخصی و حساس کاربر دسترسی پیدا کنند .

-اگر امن سازی صورت نگرفته باشد، ایمیل های فرستاده یا دریافت شده می تواند جعل یا توسط دیگران خوانده شود .

- ایمیل ها یکی از منابع ویروس ها و برنامه های مخرب هستند.

-لازم است که ایمیل ها برای ارتباطات امن و حفاظت از حریم خصوصی، ایمن شوند.

تهدیدات امنیتی ایمیل:

پیوست های مخرب ایمیل: فایل های ضمیمه ممکن است حاوی یک ویروس تروجان، کرم های keylogger و... باشد و باز کردن چنین پیوست هایی کامپیوتر را آلوده می کند

.فیشینگ : ایمیل های فیشینگ قربانیان را برای ارائه ی اطلاعات شخصی فریب می دهند.

هدایت کاربر به یک آدرس مخرب : ایمیل ها ممکن است حاوی لینک به سایت های مخرب یا دارای مطالب مربوط. به pornographicباشند

ایمیل Hoax/Chain : ممکن است کاربر ایمیل های جعلی دریافت کند که شامل اطلاعات اشتباهی است که به او می گوید نامه ای را ارسال کند.

Spamming :کاربر ممکن است ایمیلهای اسپمی را دریافت کند که حاوی نرم افزارهای مخرب باشد که به مهاجمین اجازه می دهد تا کامپیوتر کاربر را کنترل کند.

پیوست های مخرب ایمیل :

- پیوست های ایمیل تهدیدات امنیتی عمده ی ایمیل هستند، زیرا آنها ساده ترین و قویترین راه ها را برای حمله به یک کامپیوتر، به مهاجمان ارائه می دهند.

- بیشتر پیوست های مخرب، یک ویروس، تروجان، نرم افزار جاسوسی یا هر نوع دیگر از بدافزار را نصب می کنند که به زودی شما آنها را باز می کنید.

پیوست های ایمیل: هشدارها

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

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

-هرگز پیوست های ایمیل ارسال شده از منابع غیرقابل اعتماد را باز نکنید.

- قبل از باز کردن، تمام پیوست ها را ذخیره و اسکن کنید .

-پیوست های حاوی فایل هایی با پسوندهای مشکوک و ناشناخته باز نکنید. به عنوان مثال *.exe, *.vbs, *.bat, : *.ini, *.bin, *.com, *.pif, *.zzx

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

Spamming:

- استفاده از سیستم های ایمیل برای ارسال توده پیام های ناخواسته، بدون در نظر گرفتن صندوق های پستی کاربران است .

- ایمیل های اسپم ممکن است حاوی برنامه های کامپیوتری مخرب مانند ویروس ها و تروجان ها باشند .

- طبق گفته ی سیمانتک، اسپم ۸۹.۱ درصد از کل ترافیک ایمیل را تشکیل می دهد.

راه های مقابله با Spamming **:**

-ایمیل های اسپم مشکوک را گزارش کنید .

-برای ثبت نام در هر وب سایت، از آدرس ایمیل رسمی استفاده نکنید.

-هنگام ارسال پیام به هر انجمن عمومی، از یک آدرس ایمیل متفاوت استفاده کنید .از باز شدن پیام های اسپم جلوگیری کنید (مرتب شده توسط فیلترهای اسپم)

-از ابزارهای آنتی اسپم یا فیلتر اسپم کلاینت ایمیل استفاده کنید

- هرگز لینک های موجود در پیام های نکنید.

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

ایمیل های Chain/ Hoax **و** Scam

Hoaxs،پیام های هشدار در مورد تهدیدات غیرواقعی به گیرندگان ایمیل هستند .به کاربران در مورد اثرات نامطلوب ارسال نکردن آن ایمیل به دیگران هشدار داده می شود.

ایمیل Scam ،اطلاعات شخصی مانند اطلاعات حساب بانکی، شماره کارت اعتباری، رمز عبور و ... را از کاربر درخواست می کند .فرستنده ایمیل Scam ،همچنین ممکن است از گیرنده بخواهد که ایمیل را به تمام کسانی که در لیست مخاطبانش وجود دارند ارسال کند.

کلاهبرداری نیجریه ای:

•کلاهبرداری نیجریه ای یا Scam Nigerian نوعی پیش پرداخت یا انتقال پول است .

• دلیل نام گذاری این کلاهبرداری به کلاهبرداری نیجریه ای این است که ابتدا در نیجریه آغاز شده است اما می تواند در هر جای دنیا انجام شود

• با استفاده از این کلاهبرداری، کلاهبرداران با ارسال یک ایمیل و پیشنهاد یک سهم در یک سرمایه هنگفت با شما تماس می گیرند.

• .آنها می گویند که می خواهند پولی را که در طی جنگ های داخلی در بانک ها بلوکه شده است به حساب شما انتقال دهند

• .همچنین آنها ممکن است دلایل مختلفی از قبیل مشکل ارثی بزرگ، محدودیت های دولت یا مالیات در کشور کلاهبردار را ذکر

• کلاهبرداران از شما می خواهند که پول یا اطلاعات حساب بانکی خود را برای کمک به آنها در انتقال این پول ارسال کنید.

لایه های کنترل امنیت ایمیل :

- فیلترهای اکتشافی
- شناسایی زبان
- فیلترهای URL
- امضاها
- سرویس اعتبار
- لیست فرستندگان غیرمجاز
-لیست فرستندگان مجاز
-فیلترهای محتوا

روش های امنیتی ایمیل:

ایجاد و استفاده از پسورد قوی - تهیه آدرس ایمیل جایگزین برای بازیابی ایمیل - آخرین لاگین را بررسی کنید - از Httpsبرای اتصال به مرورگر استفاده کنید - گزینه هایKeep Me , Remember Me / Singed in را غیرفعال کنید یا انتخاب نکنید - پیوست ای ایمیل را جهت یافتن نرم افزارهای مخرب اسکن کنید - قابلیت پیش نمایش را خاموش کنید و تنظیمات دانلود را در کلاینت های ایمیل تغییر دهید - فیلتر ایمیل کم اهمیت را در کلاینت های ایمیل ایجاد کنید - پیام های ایمیل خود را به صورت دیجیتالی امضا کنید - با استفاده از فیلترها، از ایمیل های ناخواسته جلوگیری کنید

ایجاد پسوردهای قوی

- یک پسورد قوی و آسان برای به یاد آوردن ایجاد کنید و آن را هر جایی یادداشت نکنید
- یک پسورد قوی می تواند با ترکیبی از اعداد و حروف کوچک و بزرگ کاراکترهای خاص ساخته شود
- پسوردهای قوی برای کرک و حدس زدن دشوار هستند

آدرس ایمیل جایگزین:

•آدرس ایمیل جایگزین، یک آدرس ایمیل اضافی و ضروری است برای ثبت نام در بسیاری از سرویس های ایمیل مانند Gmail و Yahoo

•توسط ارائه دهندگان سرویس برای تایید تشخیص سازنده حساب، استفاده می شود .

• آدرس های ایمیل جایگزین برای بازیابی پسورد در صورت فراموشی، مورد استفاده قرار می گیرند .

Keep Me Signed In/Remember Me

•بیشتر کلاینت های ایمیل محبوب، گزینه های. Keep Me Remember Meیا signed in را دارند.

• بررسی این گزینه ها به کلاینت ایمیل اجازه می دهد تا صندوق پستی کاربر رت بدون پر کردن مجدد اطلاعات لاگین، بازیابی کند

• .این گزینه ها به کاربران دیگر اجازه می دهند تا به ایمیل کاربر دسترسی پیدا کنند

• .کاربران باید این گزینهها را هنگام دسترسی به ایمیل از یک کامپیوتر عمومی، انتخاب نکنند .

استفاده ازHTTPS

•حساب های کاربری ایمیل تحت وب مانند Gmail ، Yahoomail، AOL Mail و غیره یک گزینه برای انتخاب پروتکل ارتباطی برای اتصال مرورگر دارند .

•استفاده تنظیمات اتصال مرورگر را برای دریافت ایمیل با استفاده از از پروتکل Secure HTTP)HTTPS تغییر دهید.

چک کردن آخرین فعالیت حساب کاربری

در صورت در دسترس بودن این ویژگی در سرویس ایمیل، همیشه آخرین فعالیت حساب کاربری را بررسی کنید .

آخرین فعالیت حساب کاربری شامل اطلاعاتی مانند: نوع دسترسی (مرورگر، تلفن همراه و غیره)، موقعیت (آدرس IP)و تاریخ و زمان فعالیت های حساب کاربری است .تهدیدات مربوط به امنیت سیستم پخش بدافزار امنیت سیستم دستورالعمل های ابزارهای امنیتی ویندوز، امنیت رمز عبور امنیت ایمیل امنیتی ویندوز چک لیست ها Detailsکلیک کنید. برای بررسی فعالیت حساب کاربری در Gmail به پایین صفحه بروید و روی در صورت مشاهده هر فعالیت مشکوک، بلافاصله پسورد و نشانه های آن را تغییر دهید .

اسکن کردن پیوست های ایمیل:

•هنگام باز کردن هر پیوست ایمیل احتیاط کنید

• .همه ی فایل های پیوست را ذخیره کنید و آنها را قبل از باز کردن، با استفاه از یک آنتی ویروس جهت یا فتن بدافزارها اسکن کند

•. فعال کردن آنتی ویروس به طور خودکار همه ی ایمیل ها و دانلودها را اسکن می کند .

خاموش کردن ویژگی پیش نمایش:

•کلاینت های ایمیل یک گزینه برای ارائه ی پیش نمایشی از ایمیل دارند

• .این ویژگی ایمیل را در کلاینت های ایمیل خاموش کنید

• .با فعال کردن این ویژگی ممکن است بدون اینکه پیام را باز کنید یک کد اسکریپت اجرا شود

• .برای خاموش کردن ویژگی پیش نمایش در :Microsoft Outlook به منوی View بروید و Pane Reading را انتخاب کنید بر روی گزینه Off کلیک کنید.

•برای خاموش کردن این ویژگی در :Mozilla Thunderbbird . به منوی View بروید و Layout را انتخاب کنید گزینه ی Pane Message را غیرفعال کنید

فیلتر کردن ایمیل: اجتناب از ایمیل های ناخواسته

•فیلتر کردن ایمیل فرایند سازماندهی ایمیل ها براساس یک معیار مشخص است

• .فیلترهای ایمیل معمولا برای شناسایی و دسته بندی ایمیل های اسپم استفاده می شوند

• .برای جلوگیری از ایمیل های ناخواسته در Outlook۲۰۱۰ ،در منوی Home به قسمت Delete group بروید، روی گزینه ی Junkو سپس Junk e-mail Options کلیک کنید، در منوی Blocked Sender ،روی گزینه ی Add کلیک کنید

• .یک آدرس ایمیل ی نام دامنه وارد کنید و روی گزینه ی OK کلیک کنید

امضای دیجیتالی ایمیل ها:

•امضاهای دیجیتال برای تایید هویت فرستنده یک پیام یا امضا کننده یک داکیومنت، استفاده می شوند

• .همچنین می توانند برای اطمینان از اینکه محتوای اصلی پیام تغییر نکرده است، مورد استفاده قرار گیرند

• .کاربران به یک گواهینامه ایمیل برای امضای دیجیتالی ایمیل ها نیاز دارند

• می توانید امضاهای دیجیتال را از متصدیان صدور گواهینامه دریافت کنید

نحوه دریافت گواهینامه دیجیتال

• .به وب سایت متصدیان صدور گواهینامه مراجعه کنید

• .یک گوهینامه دیجیتال را خریداری و دانلود کنید

• .برخی از متصدیا صدور گواهینامه، گواهینامه رایگان ارائه می دهند

•Comodo .یک نمونه از گواهینامه های امنیتی ایمیل است اطلاعات شخصی را برای دانلود گواهینامه، ارئه دهید

• .به حساب کاربری ایمیل خود که هنگام دانلود گواهینامه ارائه دادید، لاگین کنید

• .صندوق پستی خود را جهت مشاهده لینک نصب گواهینامه، بررسی کنید .

نصب یک گواهینامه دیجیتال

•برای نصب گواهینامه دیجیتال روی لینک نصب کلیک کنید..

• در مرورگر اینترنت اکسپلورر، به مسیر زیر برویدTools - Internet Options - Content tab

• :درContent tab روی دکمه Certificates کلیک کنید

• .گواهینامه را انتخاب کنید و روی دکمه Export کلیک کنید

• .روی دکمه Next کلیک کنید

•Yesرا انتخاب کنید private key را اکسپورت کنید

• .روی Next کلیک کنید

• .از private key با دادن یک پسورد و confirm آن، محافظت کنید

• .فایل مورد نظر خود برای اکسپورت را انتخاب کرده و آن را در یک مکان خاص ذخیره کنید .

امضا کردن ایمیل ها:

- به مسیر زیر بروید Microsoft Outlook - File - Option

- به ترتیب روی دکمه های زیر کلیک کنید: Trust Center- Trust Center Setting- Email Security

-با انتخاب check boxes مناسب در زیر بخش Encrypted e- mail ایمیل را رمزگذاری کنید

-روی دکمه Import یا Export کلیک کنید

- با انتخاب دکمه Browse ،فایل را باز کنید و پسورد و شناسه نام دیجیتال را وارد کنید .

- روی دکمه OK کلیک کنید

- • برای نوشتن یک پیام، روی دکمه New Mail کلیک کنید

- پس از کلیک روی دکمه send رمزگذاری پیام آغاز خواهد شد .

- روی دکمه Send Unencrypted کلیک کنید (اگر گیرندگان private key ندارند)
- اگر گیرندهprivate key دارد روی دکمه Continue کلیک کنید .
•در بخش Trust Center ،روی بخش Automatic Download کلیک کنید

سیستم آنلاین رمزگذاری ایمیل Lockbin :

- Lockbinیک سرویس رایگان برای ارسال ایمیل های محرمانه است

-این سیستم برای ارسال اطلاعات محرمانه مانند جزئیات کارت اعتباری و اطلاعات کسب و کار، استفاده می شود .

خلاصه:

-ایمیل یک روش تبادل پیام های دیجیتال از یک فرستنده به یک یا چند گیرنده است .

- فایل های ضمیمه (پیوست ها) می توانند حاوی برنامه های مخرب باشند، که باز کردن چنین پیوست هایی می تواند کامپیوتر را آلوده کند .

- Spamming فرایند اشغالکردن صندوق ورودی کاربر با ایمیل های ناخواسته و بی ارزش است .

- Hoaxes هشدارهای دروغین با ادعای گزارش های مربوط به یک ویروس غیرواقعی هستند .

- تنظیمات تلفن همراه را فقط برای دانلود header ایمیل ها در نظر بگیرید نه برای تمام ایمیل

- پاک کردن Cache ،پسوردها و history مرورگر را فراموش نکنید .

- امضاهای دیجیتال برای تایید هویت فرستنده یک پیام یا امضا کننده یک داکیومنت، استفاده می شوند .

- ابزارهای امنیتی ایمیل از پسوردها و خروج خودکار از حساب های کاربردی ایمیل، محافظت می کنند

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 .

-پیام ها را براساس الویت، موضوع، تاریخ، فرستنده و دیگر موارد مرتب کنید.

-این کار به شما در جستجوی ایمیل ها کمک می کند .

-صندوق وردوی خود را مرتبا پاک کنید. از ارسال اطلاعات محرمانه، حساس، شخصی و طبقه بندی شده در ایمیل ها اجتناب کنید .

-پوشه هایی را ایجاد کنید و ایمیل ها را براساس خانواده، دوستان، کار و غیره به آنها انتقال دهید .

-ایمیل هایی را که ارسال می کنید، به صورت دیجیتالی امضا کنید .

چک لیست امنیتی برای بررسی ایمیل ها در موبایل :

تنظیمات موبایل برای دانلود Header ایمیل ها در نظر بگیرید نه برای تمام ایمیل فایل های پیوست بزرگ را از طریق موبایل، ارسال و باز نکنید .

یک آنتی ویروس موبایل نصب کنید و آن را آپدیت نگه دارید.

لینکهایی که توسط ایمیل یا پیام های متنی فرستاده شده اند، دنبال نکنید .

گزینه نمایش تصاویر را در مرورگر موبایل خود غیرفعال کنید .فایل های مهم را به صورت Zip ارسال کنید.

برای کاهش اندازه ایمیل، آنها را یک متن ساده ارسال کنید .