ویروس

امروزه پیشرفته شدن جوامع و گسترش تکنولوژی بیشتر ارتباطات از این طریق انجام میگیرد، به موازات این پیشرفت هر روزه ویروس ها و بدافزار های متعددی برای آسیب رساندن به سیستم ها و سرقت اطلاعات آن توسط برنامه نویسان تولید میشود. با رعایت نکات ساده ای میتوانید تا حد بسیار زیادی از خطر این نوع حملات در امان باشید.

ابتدا باید راه های ویروسی شدن کامپیوتر خود را بشناسید.

آشنایی با کلاهبرداری شایع در اینترنت به نام (Phishing)

فیشینگ روشی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶رقمی عابر بانک، رمز دوم و CVV۲ را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می برند. شبکه های اجتماعی، سایت های حراجی و درگاه های پرداخت آنلاین نمونه ای از ابزار های الکترونیکی ارتباطات می باشند.

کلاهبرداری فیشینگ از طریق ایمیل ها و پیام ها صورت می پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در وب سایت های جعلی که در ظاهر کاملا شبیه وب سایت های سالم و قانونی می باشد وارد می نمایند. حقه ی فیشینگ یکی از تکنیک های مهندسی اجتماعی برای فریب کاربران می باشد که علی‌القاعده از ضعف امنیتی یک وب سایت برای انجام عملیات مجرمانه خود استفاده می کنند؛ برای اولین بار حقه ی فیشینگ در ۱۹۸۷ تعریف شد و اولین باری که واژه فیشینگ برای نام گذاری این واژه استفاده گردید، سال ۱۹۹۶ بود.

جالب است بدانید phishing نوع دیگر کلمه fishing (ماهیگیری) است همانند خیلی از کلمات که در علوم رایانه ای به شکل مخفف یا دگرگون شده ای از کلمات دیگر به کار می روند. برای مثال لغت phreak که از ترکیب phone freak به معنای استراق سمع تلفنی گرفته شده است .با این توضیحات شاید بتوان phishing را سرقت اطلاعات اینترنتی با یک سایت قلابی ترجمه کرد.

کلاهبرداری فیشینگ چگونه انجام می شود؟

ممکن است سارق با یکی از اعضای سایتی که در آن خرید و فروش صورت می گیرد روبرو شود و پیام کوتاهی برای او مبنی بر وارد کردن رمز عبور بفرستد.برای اینکه قربانی احتمالی خوب به دام بیفتد آن پیام کوتاه ممکن است به صورت یک عبارت امری مانند این « اطلاعات صورتحساب را تأیید کنید» باشد. به محض اینکه قربانی رمز عبور خود را وارد کند شخص سارق می تواند به حساب طرف وارد شده و از آن برای انجام اهداف مجرمانه ی خود استفاده کند. البته این کار احتیاج به دانش برنامه نویسی دارد.

فیشینگ در سایت AOL.com به قدری به وفور اتفاق افتاد که مسوولین سایت مجبور شدند در سایت خود نواری با این توضیح که "هیچ یک از مسوولان در این سایت از شما درخواست رمز نخواهند کرد" قرار دهند .

From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

این قسمت را برای تأیید حساب خود کلیک کنید

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

در تصویر بالا می توانید یک ایمیل جعلی (phishing Email) مشاهده کنید که کاربران سایت PayPal را مورد هدف قرار داده است؛ ۳ مورد غلط املایی و آدرس IP ظاهر شده در زیر لینک درون کادر باریک مستطیلی نشانه هایی از قلابی بودن این صفحه هستند.

در اواخر سال ۲۰۰۶ یک کرم رایانه ای کنترل سایت MySpace را بدست آورد و تمام لینک های دانلود فایل ها را به سوی سایت هایی که برای دزدیدن اطلاعات حساب های اینترنتی درست کرده بود تغییر مسیر داد.

چگونه با اطمینان خاطر،خرید خود را از طریق اینترنت انجام دهیم؟

چگونه در اینترنت به خرده فروشان اعتماد کنیم و در دام دسیسه های کلاهبرداری نیافتیم؟ هر روز میلیون ها نفر بدون هیچ گونه مشکلی در اینترنت خرید می کنند. با داشتن کمی شجاعت و دانش، شما می توانید از ایجاد مشکلات مربوط به تجارت الکترونیکی جلوگیری نمائید .

خطرات:

- خرید کالاهایی که تحویل داده نمی شوند.
- ارائه کالاهایی که با خصوصیات گفته شده در سایت مطابقت ندارند.
- تاخیر ها و زحمت هایی که خرید آنلاین دارد.
- خدمات ضعیف پس از فروش
- سوء استفاده از کارت های اعتباری شما

با فروشندگان مطمئن و معروف معامله کنید:

•فروشندگان دارای اعتبار را انتخاب کنید. مخصوصاً زمانی که از اشخاص خاصی خرید می کنید.

•در جستجوی مدارک واقعی مانند جزئیات آدرس و شماره تلفن برای برقراری ارتباط باشید.

•فقط با بازدید از وب سایت افراد یا شرکت ها در مورد آنها قضاوت نکنید.

•وقتی که در حال خرید از شرکت های خارجی هستید، به طور خاص خیلی حساس باشید.

•سیاست فروشندگان در حفظ حریم شخصی و بازپرداخت مبلغ کالا را بررسی نمائید.

•از روش های مناسب و ایمن برای پرداخت پول در اینترنت استفاده کنید تا در صورت عدم تحویل کالا از اطلاعات مالی و بانکی شما تا حدی محافظت شود.

از یک وب سایت مطمئن استفاده کنید.

•اطمینان حاصل کنید که از یک وب سایت مطمئن برای وارد کردن اطلاعات کارت اعتباری خود استفاده می کنید. در گوشه پایین سمت راست پنجره مرورگر خود به دنبال نشانه ای از قفل (Padlock) باشید و اطمینان حاصل کنید که آدرس وب سایت با (https://)آغاز می شود.

•اگر شما از آخرین نسخه مرورگر خود استفاده می کنید و وب سایت اینترنتی فروشگاه از جدیدترین تکنولوژی امنیتی مانند نسخه جدید و معتبر شناسه امنیتی SSL استفاده می کند، ممکن است وقتی که از یک وب سایت مطمئن بازدید می کنید، نوار آدرس شما سبز شود.

•اگر اخطاری در ارتباط با شناسه امنیتی سایت دریافت کردید، خیلی حساس و محتاط باشید. در هر حال، قفل (Padlock) نشانه ای دقیق از وجود امنیت در سایت نیست و هیچ ارتباطی با اصول اخلاقی مورد استفاده صاحبان سایت ندارد .

•بر روی قفل (Padlock) کلیک کنید تا بتوانید ادعای فروشنده در مورد هویتش را ببینید و بررسی کنید که آیا شناسه امنیتی آنها در آدرس درست و واقعی ثبت شده است یا خیر.

•اطلاعاتی که توسط قفل (Padlock) روی صفحه ظاهر می شود، نباید شما را فریب دهد. برای صاحبان اصلی سایت کپی کردن تصویر یک قفل (Padlock) کار آسانی است. شما باید به دنبال قفلی (Padlock) باشید که در پنجره اصلی خود مرورگر وجود دارد .

از دسیسه های کلاهبرداری بر حذر باشید.

•اگر شرایط (یک معامله) خیلی بیشتر از حد واقعی ،عالی به نظر برسد، احتمالاً حقه ای در کار است. در اینترنت به بررسی اطلاعات راجع به این شرکت بپردازدید و بررسی کنید که آیا شخصی قبلاً با این مشکل مواجه شده است .

•از طرح های کار در خانه که وعده می دهند به راحتی می توانید درآمد کسب کنید و هیچ وقت هزینه ای نپردازید، اجتناب کنید .

•از شرکت های معتبر خرید کنید.

•به شدت از هر چیزی که در پیام های ناخواسته یا هرزنامه ها (Spam) ارائه و تبلیغ می شود، اجتناب و دوری کنید .

فروش آنلاین

اگر شما شرکتی دارید که بخش فروش آنلاین دارد،:

•مشتریان و عرضه کنندگان جدید را از طریق اطلاعات منتشر شده در مورد آنها (مانند شماره تلفن یا آدرس) شناسایی کنید.

•قبل از ارسال هر نوع کالایی به صورت نسیه، گزارشی از وضعیت اعتباری مشتریان خود تهیه کنید.

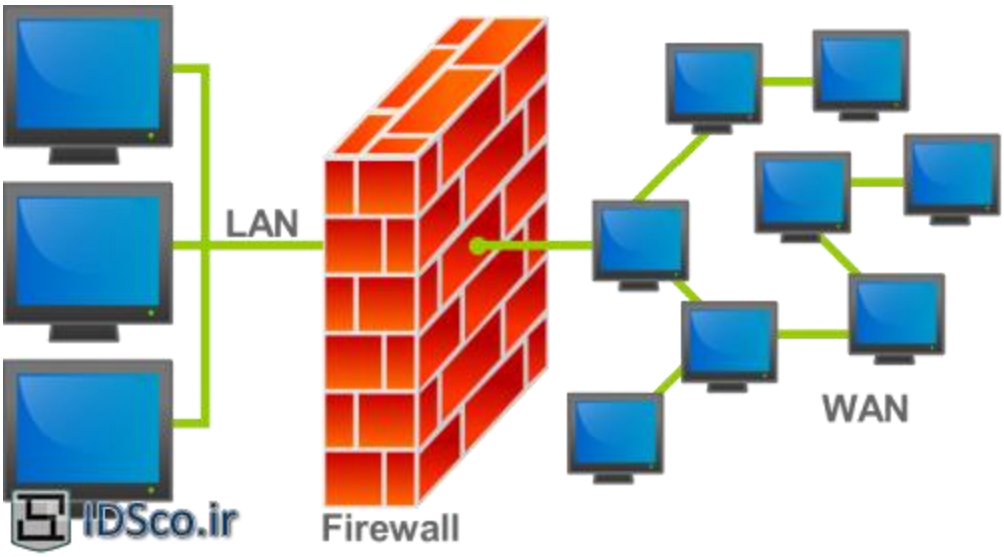
•شرکت های تجارت الکترونیک در قبال هر نوع کلاهبرداری از کارت های اعتباری مسئول هستند. (مگر آن که آنها از خدمات Verified by Visa)شرکت های تایید شده توسط(Visa یا)MastercardSercurecode کد امنیتی (Mastercardاستفاده کنند. این سیستم ها از شرکت ها در برابر اتهامات کلاهبرداری، حمایت می کنند(.

•استفاده از سیستم های بررسی هویت و اعتبار آدرس (AVS) و شماره امنیتی کارت (CSC) می تواند به گونه ای موثر خطرات تقلب و کلاهبرداری در تجارت الکترونیک را کاهش دهد.

•تایید اعتبار مشتری پرداخت مبلغ پول را تضمین نمی کند و بنابراین شرکت ها باید تمامی بررسی ها برای تایید اعتبار مشتری و آدرس مشتری برای تحویل کالا را انجام دهند.

دیواره های آتش (Firewall) چیست؟

دیواره آتشین (Fire wall) سیستمی است بین کاربران یک شبکه محلی و یک شبکه بیرونی) مثل اینترنت) که ضمن نظارت بر دسترسی ها، در تمام سطوح، ورود و خروج اطلاعات را تحت نظر دارد. بر خلاف تصور عموم کاربری این نرم افزارها صرفاً در جهت فیلترینگ سایت ها نیست.



برای آشنایی بیشتر با نرم افزارهای دیواره های آتشین، آشنایی با طرز کار آنها شاید مفیدترین راه باشد. در وهله اول و به طور مختصر می توان گفت بسته های TCP/IP قبل و پس از ورود به شبکه وارد دیواره آتش می شوند و منتظر می مانند تا طبق معیارهای امنیتی خاصی پردازش شوند.

●حاصل این پردازش احتمال وقوع سه حالت است :

۱ (اجازه عبور بسته صادر می شود.

۲ (بسته حذف می شود.

۳ (بسته حذف می شود و پیام مناسبی به مبدا ارسال بسته فرستاده می شود.

●ساختار و عملکرد

با این توضیح، دیواره آتش محلی است برای ایست بازرسی بسته های اطلاعاتی به گونه ای که بسته ها براساس تابعی از قواعد امنیتی و حفاظتی پردازش شده و برای آنها مجوز عبور یا عدم عبور صادر شود. همانطور که همه جا ایست بازرسی اعصاب خردکن و وقت گیر است دیواره آتش نیز می تواند به عنوان یک گلوگاه باعث بالا رفتن ترافیک، تاخیر، ازدحام و بن بست شود.

از آنجا که معماری TCP/IPبه صورت لایه لایه است (شامل ۴ لایه: فیزیکی، شبکه، انتقال و کاربردی) و هر بسته برای ارسال یا دریافت باید از هر ۴ لایه عبور کند بنابراین برای حفاظت باید فیلدهای مربوطه در هر لایه مورد بررسی قرار گیرند. بیشترین اهمیت در لایه های شبکه، انتقال و کاربرد است چون فیلد مربوط به لایه فیزیکی منحصر به فرد نیست و در طول مسیر عوض می شود. پس به یک دیواره آتش چند لایه نیاز داریم. سیاست امنیتی یک شبکه مجموعه ای از قواعد حفاظتی است که بنابر ماهیت شبکه در یکی از سه لایه دیواره آتش تعریف می شوند .

●کارهایی که در هر لایه از دیواره آتش انجام می شود عبارت است از:

۱ (تعیین بسته های ممنوع (سیاه) و حذف آنها یا ارسال آنها به سیستم های مخصوص ردیابی (لایه اول دیواره آتش(

۲ (بستن برخی از پورت ها متعلق به برخی سرویس ها مثلTelnet، FTPو... (لایه دوم دیواره آتش(

۳ (تحلیل برآیند متن يك صفحه وب یا نامه الکترونیکی یا .... (لایه سوم دیواره آتش(

آموزش کامل و جامع استفاده از مرورگر internet explorer

ظاهرا ، مهم ترین مطلب در مورد برنامه internet explorer این است که این مرورگر به تنهائی یک برنامه نیست ، اما با استفاده از این مرورگر به منابع زیادی دست پیدا می کنید و باید کاملا در مورد آن اطمینان داشته باشید .
استفاده از برنامه internet explorer ، به حدی آسان است که به ندرت نیاز به یک کتاب مبانی ، و حتی به این فصل دارید.
اگر بدانید که چگونه یک برنامه را در ویندوز XP حرفه ای می توان باز کرد ، پس می دانید که چگونه برنامه internet explorerرا باز کنید ، و به آسانی با کلیک بر روی لینک ها ، می توانید فورا گشت و گذار خود را شروع کنید.
بنابراین من قصد دارم در این فصل تمام کار هائی را که عموما با internet explorer انجام می دهید را فورا به شما انتقال دهم همانند گذشته ، به تعدادی از ویژگی های جدید نسخه ، اشاره خواهم کرد و نشان می دهم که چگونه می توان چیزها یی را که به طور طبیعی می آیند ، گسترش داد .

مثلا احتمالا می دانید که برای دستیابی به یک منبع اینترنتی باید در قسمت منوی آدرس ، URLآن منبع را وارد کنید . این کار در مواردی مانند www.microsoft.com خیلی آسان است اما در مورد
?۱hsp+yhoo&d-v۱http://finance.yahoo.com/q?s=msft+brka+csco+ald+mmm+sci+
چطور ؟ در این فصل خواهید دید که در برنامه internet explorer حد اقل نیم دو جین راه و روش وجود دارد ، تا به یک URLمفصل و تولانی دست پیدا کنید و حتی می توان بدون تایپ کردن به URL دسترسی پیدا کرد.

خبر خوب این روزها این است که قیمت کامپیوتر های شخصی در حال سقوط است و مرورگرهائی مانند internet explorer آسان تر استفاده می شوند و قدرتمند ترند . تنها خبر بد این است که بیشتر ما معمولا در طول روز وقت کافی نداریم تا به ظواهر و فروانیهای اینترنت نگاهی بیندازیم . اگر چه ، شما می توانید در اینجا مهارتهائی را کسب کنید تا فعالیتهایتان را کار آمد کرده و از وقتتان استفاده بیشتری ببرید.

۱ – شروع کار با internet explorer

۲ – گردشی درinternet explorer

۳ – حرکت در وب

۴ – پیدا کردن آنچه شما در اینترنت می خواهید

۵ – شفارشی کردن برنامه internet explorer