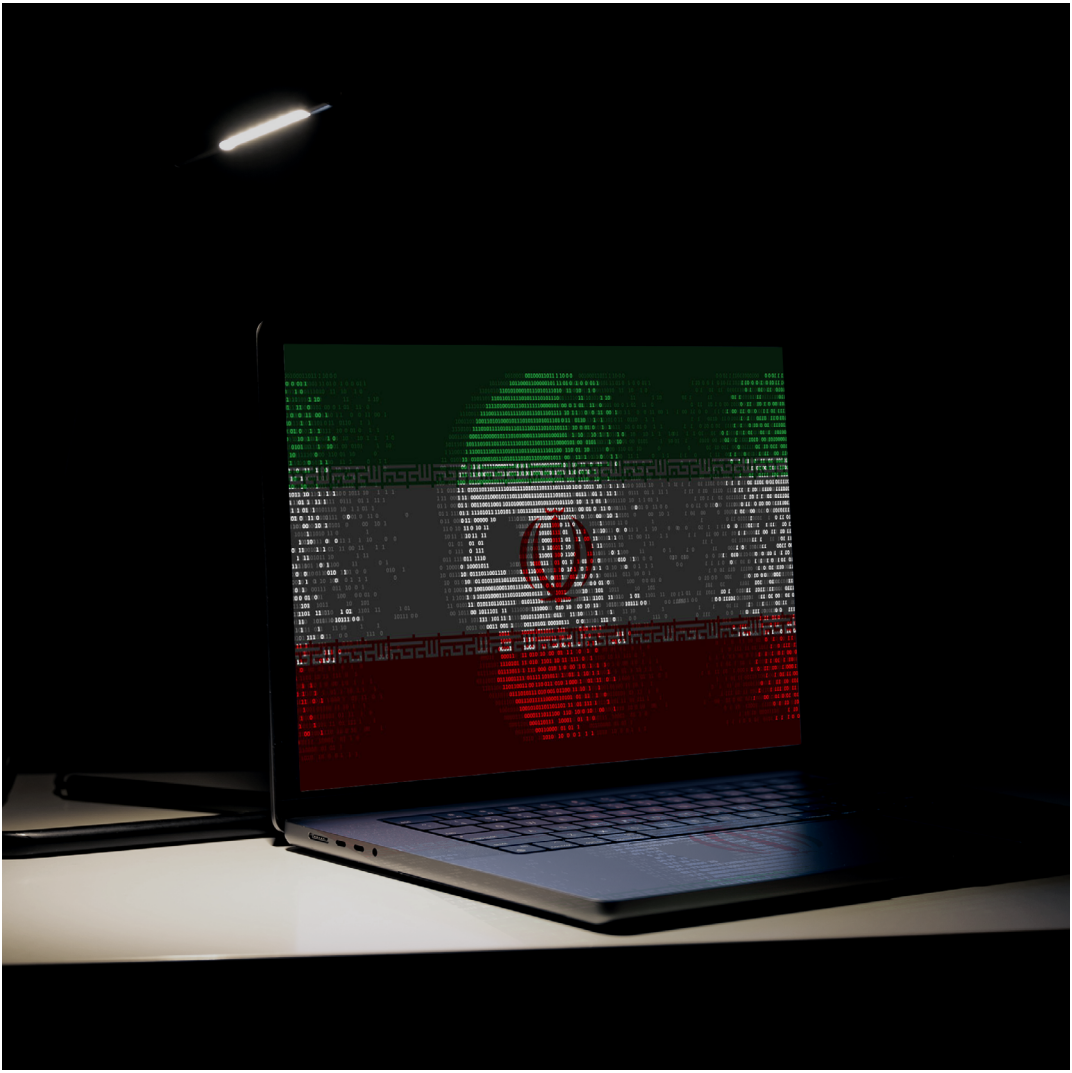

روش‌های مقابله با حملات سایبری

ویژه کنشگران

توانا TAVAANA

روش‌های مقابله با حملات سایبری

ویژه کنشگران

توانا
TAVAANA
آموزشکده آنلاین برای جامعه مدنی ایران
e-collaborative
for civic education

https://tech.tavaana.org

پروژهٔ

e-collaborative
for civic education

www.eciviced.org

روش‌های مقابله با حملات سایبری

ویژه کنشگران

ناشر: E-Collaborative for Civic Education

پاییز ۱۴۰۳

---

e-collaborative
for civic education

ECCE (E-Collaborative Civic Education) یک سازمان غیرانتفاعی در ایالات متحده آمریکا تحت 501c3 است که از فناوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیان‌گذاران و مدیران این سازمان اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از جامعه سیاسی دموکراتیک پایه و اساس کار است؛ همان‌طور که حقوق عام بشر که هر شهروندی باید از آن‌ها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک‌تک شهروندان و امنیت، برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار است که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند.

ما پروژه اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعه مدنی ایران» را در سال ۲۰۱۰ تاسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس‌ماندن دانشجویان، به یک جامعه آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وب‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زنده دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با کنشگران و روشنفکران، دستورالعمل‌های خودآموز، کتابخانه مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاوره آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعه توانایی‌های آموزشکده توانا متوجه گردآوردن بهترین متفکران ایران و صداهای حذف‌شده است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان در جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فناوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هم‌وطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما!

فهرست

مقدمه

در این عصر دیجیتال که از جمله اصلی‌ترین خصایص زندگی کنونی بشر است، اینترنت بخش گسترده‌ای از زندگی‌ها را به خود اختصاص داده است. هرچند که این فضا برای افزایش ارتباطات و ارائه خدمات به کاربران بسیار مفید است، اما در کنار این مزیت‌ها، شاهد رشد حملات سایبری مختلف به کنشگران زمینه‌های مختلف هستیم؛ به‌ویژه کنشگرانی که در حوزه‌های مدنی فعالیت می‌کنند و به‌ویژه در کشورهایی مانند ایران که این مشکلات بسیار بیش‌تر نمود دارند.

امنیت دیجیتال برای کنشگرانی که از فضاهای آنلاین برای انتشار دیدگاه‌هایشان و اطلاع‌رسانی استفاده می‌کنند، بسیار اهمیت دارد. به این علت روشن که حملات سایبری می‌تواند به فعالیت آن‌ها آسیب‌های جدی وارد کند و موجب ایجاد اختلال در کنشگری‌ها شود.

برای مقابله با این حملات، کنشگران بایستی با ابزارهای امنیتی و روش‌های مقابله با حملات سایبری آگاه باشند و توانایی مقابله با این حملات را به دست بیاورند. در همین راستا، در این کتابچه به بررسی حملات سایبری مطرح برای کنشگران حوزه‌های مختلف می‌پردازیم و راهکارهایی که می‌توانند برای مقابله با این حملات به کار برده شوند را بررسی می‌کنیم.

امیدواریم مطالب این کتابچه در زمینه آگاهی‌بخشی به فعالان حوزه‌های مختلف

سودمند باشد و دانش کنشگران در زمینه‌هایی چون امنیت دیجیتال، حملات سایبری و نوع مقابله با حملات سایبری را افزایش دهد.

تعریف حملات سایبری

حملات سایبری به معنای نفوذ هدفمند به سیستم‌های کامپیوتری، شبکه‌ها، سرویس‌های آنلاین، دستگاه‌های متصل به اینترنت و سایر منابع دیجیتال است. این حملات معمولا توسط افراد یا گروه‌هایی برای دسترسی غیرمجاز به اینترنت و فناوری‌های مرتبط انجام می‌شوند.

هدف اصلی حملات سایبری می‌تواند دستیابی به اطلاعات حساس و سرقت اطلاعات شخصی یا مالی باشد یا تخریب و ایجاد اختلال در عملکرد سیستم‌ها یا سرقت محتوا و مالکیت فکری. تامین منابع مالی غیرقانونی، نفوذ به سیستم‌های دیگر به عنوان نقطه شروع برای حملات دیگر یا تلاش برای تاثیرگذاری سیاسی، اقتصادی و اجتماعی از دیگر انواع اهداف حملات سایبری به شمار می‌روند.

حملات سایبری می‌توانند انواع مختلفی از تهدیدات را شامل شوند؛ حملات نفوذ، کرم‌ها و ویروس‌ها، حملات DDOS[1]، فیشینگ، حملات به شبکه‌های اجتماعی اشخاص و البته انواع فراوان دیگری که ذکر همه آن‌ها در این مجال نمی‌گنجد. این حملات می‌توانند توسط هکرها، کلاهبرداران اینترنتی، سازمان‌های جاسوسی و گروه‌های تروریستی انجام شود و اساسا هر فردی که در جهت خلاف قانون اقدام به این کار می‌کنند.

مبارزه با حملات سایبری و ایجاد امنیت دیجیتال نیازمند اقدامات فنی، قانونی و

1. Distributed Denial Of Service Attack.

آموزشی است. بنابراین اساسا در آغاز بایستی به این بپردازیم که چرا ممکن است این حملات گریبانگیر کنشگران شود؟

چرا کنشگران مورد حمله هکرها قرار می‌گیرند؟

فعالان ممکن است به دلایل مختلفی هدف حملات هکرها قرار گیرند که در ادامه به بررسی تعدادی از این دلایل می‌پردازیم:

دسترسی به اطلاعات شخصی و حساس

فعالان اجتماعی-سیاسی ممکن است دسترسی به اطلاعات حساس و مهم داشته باشند. این اطلاعات می‌تواند شامل برنامه‌ها، راهبردها، ارتباطات و اطلاعات شخصی و سیاسی باشد. هکرها به دنبال سرقت این اطلاعات هستند تا از آن‌ها به نفع خود استفاده کنند، اطلاعات را منتشر کنند یا برای تهمت به فعالان از آن‌ها بهره بگیرند.

اهداف سیاسی

فعالان سیاسی و اجتماعی که در حوزه‌هایی مانند حقوق بشر، دموکراسی، آزادی بیان و مبارزه با سرکوب نظام‌های سیاسی اقتدارگرا فعالیت می‌کنند، ممکن است به دلیل عقاید و فعالیت‌هایشان بیش‌تر از دیگران به دام حملات هدفمند هکرها برای سرقت اطلاعات یا سرقت هویت بیفتند.

تضعیف اعتبار و تشویش فعالیت‌ها

حملات هکرها ممکن است برای تشویش فعالیت‌های فعالان و تضعیف اعتبار آن‌ها انجام

شود. به این ترتیب که حمله‌کنندگان با انتشار اطلاعات غلط، تقلبی یا تحریف‌شده، سعی می‌کنند اعتبار و قدرت فعالان را متضرر کنند و باعث شک و تردید درباره اعمال و اهداف آن‌ها در جامعه شوند.

اثرگذاری در نتیجه فعالیت‌ها

از آن جا که فعالان ممکن است در رقابت‌های سیاسی یا اجتماعی دخالت داشته باشند، هکرها تلاش می‌کنند با حملات سایبری به فعالان، نتایج و عملکرد آن‌ها را تحت تاثیر قرار دهند، اطلاعات را تغییر دهند یا حتی سیستم‌ها را تخریب کنند تا بر این فعالیت‌ها اثر بگذارند.

سانسور و محدودیت دسترسی

برخی از حکومت‌ها و نهادهای قدرتمند تلاش می‌کنند فعالان را سانسور کنند و در روند دسترسی آزاد به اطلاعات مطلوب‌شان محدودیت ایجاد کنند. در این صورت، هکرها به دنبال نفوذ به سیستم‌ها و ارتباطات فعالان هستند تا آن‌ها را شناسایی و مسدود کنند.

اثرات حملات سایبری بر کنشگران حوزه‌های مدنی

حملات سایبری روی فعالان می‌تواند اثرات مخربی داشته باشد. در ادامه به برخی از این اثرات اشاره می‌کنیم:

ازدست‌دادن داده‌های مهم و حساس

حملات سایبری می‌توانند منجر به ازدست‌دادن اطلاعات حساس شخصی و حریم خصوصی فعالان شوند. اطلاعاتی که برای این کنشگران از اهمیت بالایی برخوردار است. به عنوان نمونه حملات سایبری ممکن است منجر به افشای اطلاعات شخصی، مالی یا حتی رسانه‌ای فعالان شوند که می‌تواند خسارت‌های جبران‌ناپذیر را برای آن‌ها به ارمغان بیاورد یا در برخی موارد، حملات سایبری ممکن است منجر به دسترسی به حساب‌های بانکی فعالان شود که می‌تواند برای آن‌ها خسارت مالی جدی را در بر داشته باشد.

ایجاد ترس و تعقیب

حملات سایبری به فعالان ممکن است منجر به ایجاد ترس و استرس شود، که موجب کاهش فعالیت آن‌ها و حتی منجر به خودسانسوری در میان فعالان شود.

تغییر در محتوای فعالیت کنشگران

حملات سایبری ممکن است منجر به تغییر در محتوا و پیام‌های فعالان شود که در نهایت

نارضایتی و افت اعتماد میان مخاطبان و طرفداران آن‌ها را برانگیزاند.

آسیب به اعتبار شخصی و اجتماعی

حملات سایبری به کنشگران و افشای برخی داده‌های مربوط به حریم خصوصی می‌توانند موجب آسیب به اعتبار و شهرت آن‌ها شود، که این نیز در جای خود می‌تواند موجب آسیب به اعتبار آن‌ها در میان مخاطبان و طرفداران شود.

ایجاد محدودیت در فعالیت

حملات سایبری به فعالان ممکن است موجب ایجاد محدودیت در انجام فعالیت‌هایشان برای مدتی شود. مشخصا منظور از محدودیت در اینجا مشکلات فنی و امنیتی است و کار کنشگران را با تعویق و تاخیر روبرو می‌سازد.

در مجموع، حملات سایبری به کنشگران، موجب نومیدی و خودسانسوری در میان آنان و کاهش توانایی آن‌ها در ارائه دیدگاه‌هایشان می‌شود. فضایی که موجد ترس و تعقیب است و احساس ناامنی ایجاد می‌کند. بر این اساس است که امنیت دیجیتال برای فعالان اهمیت بالایی دارد و نباید از آن غافل شد.

حملات سایبری رایج به کنشگران حوزه‌های مختلف

فعالان معمولا هدف اصلی بسیاری از حملات سایبری هستند. حملات سایبری ممکن است شامل موارد زیر باشند:

حملات فیشینگ

حملات فیشینگ یکی از رایج‌ترین حملات سایبری هستند که از طریق ارسال پیام‌های جعلی به کاربران، سعی در جمع‌آوری اطلاعات آنان دارند. در این حملات، فردی که حمله را انجام می‌دهد، با استفاده از ایمیل‌های جعلی، وب‌سایت‌های جعلی یا پیامک‌های جعلی، تلاش می‌کند فرد مورد هدف را به هم‌خوان‌کردن اطلاعات حساس و شخصی خود مانند نام کاربری، رمز عبور، شماره کارت بانکی و غیره تحریک کند. برخی از این حملات می‌توانند بسیار هوشمندانه باشند و به آسانی قابل شناسایی نباشند.

این حملات معمولا با هدف دزدیدن اطلاعات شخصی، دسترسی به حساب بانکی، فریب افراد برای پرداخت وجه به یک شخص جعلی یا دسترسی به ایمیل و حساب شبکه‌های اجتماعی انجام می‌شوند. به همین علت، لازم است که همواره از امنیت پیام‌های دریافتی خود اطمینان حاصل کنید و قبل از به‌اشتراک‌گذاشتن هرگونه اطلاعاتی، در آغاز، از صحت درخواست، اطمینان حاصل کنید.

حملات DDoS

حملات DDoS یا Distributed Denial of Service یکی از رایج‌ترین حملات سایبری هستند که با ارسال تعداد زیادی درخواست به سرورها، سعی در کاهش سرعت سایت یا سامانه‌های اینترنتی دارند و آن‌ها را برای کاربران مسدود می‌کنند. در این نوع حمله، مهاجم از چندین دستگاه یا کامپیوتر در سراسر جهان استفاده می‌کند تا به صورت همزمان به سرورها درخواست ارسال کند و سرعت سایت را کاهش دهد. این مهاجمان که هدف ایجاد اختلال در سیستم‌های آنلاین را دنبال می‌کنند، با چنین حملاتی مانع دسترسی کاربران به سایت‌ها و موجب به‌هم‌ریختن خدمات آنلاین و آسیب‌رساندن به شرکت‌ها و سازمان‌هایی می‌شوند که به‌شدت به سامانه‌های آنلاین خود وابسته هستند.

معمولا این نوع از حمله‌های سایبری برای افرادی که سایت شخصی برای انتشار محتوا یا نقطه‌نظرهای خود دارند، بسیار رایج است. همچنین این حملات در سایت‌های موسسه‌های حوزه‌های مختلف - مخصوصا در حیطه حقوق بشری - به صورت بسیار گسترده‌تری انجام می‌پذیرد. برای مقابله با حملات DDoS، شرکت‌ها و سازمان‌ها می‌توانند از راهکارهایی مانند استفاده از فایروال‌ها، توزیع بار[1] یا Load balancing استفاده کنند یا از سرویس‌های محافظت از حملات DDoS بهره بگیرند.

حملات ویروس‌ها و بدافزارها

حملات کرم، ویروس و بدافزارها در اصل به دو نوع تقسیم می‌شوند. اولین نوع به صورت مستقیم به سیستم شما وارد می‌شوند و سعی در تغییر و ازبین‌بردن فایل‌ها و اطلاعات شما دارند. در این نوع حمله، فایل‌های مخرب می‌توانند به صورت پیام‌های ایمیل، نرم‌افزارهای شبیه‌سازی و بازی‌های آنلاین در سیستم شما قرار گیرند.

دومین نوع حمله به سیستم شما به شکل پنهان صورت می‌گیرد. این نوع حمله به عنوان «تروجان» شناخته می‌شود. تروجان‌ها می‌توانند در صورت ورود به سیستم، اطلاعات شما را گردآوری کنند، تصاویری از صفحه نمایش شما ضبط کنند و همچنین کنترل سیستم شما را از راه دور به‌دست گیرند.

---

۱ . توزیع بار به معنای تقسیم‌بندی درخواست‌ها و ترافیک بین منابع مختلف سیستم است تا بار به صورت متوازن و منظم توزیع شود.

با توجه به این‌که کرم‌ها و ویروس‌ها به صورت پنهانی و مخفیانه عمل می‌کنند، بسیار دشوار می‌توان آن‌ها را شناسایی کرد و از بین برد. به علاوه با پیشرفت فناوری، کرم‌ها و ویروس‌های جدید و پیچیده‌تری به وجود می‌آیند که موجب افزایش امنیت سیستم‌های اطلاعاتی می‌شوند. بنابراین، حفاظت از سیستم‌های شخصی و سازمانی بسیار مهم است.

حملات نفوذ یا Intrusion attacks

این نوعی از حمله است که در آن حمله‌کننده با بهره‌گیری و شناسایی آسیب‌پذیری‌های موجود در سیستم، راه نفوذ به سیستم و شبکه کامپیوتری شما تدارک می‌بیند و به اطلاعات‌تان دست پیدا می‌کند. حملات نفوذ معمولا توسط افرادی انجام می‌شوند که دانش فنی خوبی دارند و با استفاده از ابزارهای مختلف، سعی می‌کنند به سیستم‌ها و شبکه‌های شما نفوذ کنند.

در بسیاری از موارد، حملات نفوذ برای دسترسی به اطلاعات حساس و مهمی همچون اطلاعات بانکی، اعتبارات اینترنتی و اطلاعات شرکت‌ها انجام می‌شوند. با توجه به اهمیت و حساسیت اطلاعاتی که ممکن است در اختیار حمله‌کننده قرار گیرند، حملات نفوذ یکی از خطرناک‌ترین حملات سایبری برای فعالان محسوب می‌شوند. به همین دلیل افراد و سازمان‌ها باید از روش‌های مختلفی همچون رمزنگاری، استفاده از نرم‌افزارهای امنیتی و بررسی مستمر وضعیت امنیتی سیستم‌ها و شبکه‌های خود، برای مقابله با این نوع حملات استفاده کنند.

حملات پیام‌رسان‌ها

حملات پیام‌رسان‌ها دقیقا شبیه حملات فیشینگ هستند با این تفاوت که از طریق پیام‌رسان‌ها انجام می‌شوند. در حملات پیام‌رسان‌ها، حمله‌کننده اغلب با استفاده از فریب و با دستکاری در پیام‌های خود، تلاش می‌کند تا به اطلاعات شخصی شما دسترسی پیدا کند یا موجب شود که شما ناخواسته عملی انجام دهید که به ضررتان تمام شود. برای مثال حمله‌کننده می‌تواند یک پیام جعلی به شما ارسال کند؛ پیامی که به نظر می‌رسد مربوط به یک سرویس یا شرکت معتبر است و در قالب آن از شما خواسته می‌شود تا به صفحه‌ای وارد شوید و اطلاعات کاربری خود را وارد کنید. در این صورت، حمله‌کننده

می‌تواند به‌راحتی به اطلاعات شما دسترسی پیدا کند.

به همین ترتیب حمله‌کننده ممکن است با استفاده از پیام‌هایی که به نظر می‌رسد از یک منبع معتبر فرستاده شده، شما را به بازکردن فایل‌هایی که حاوی بدافزار هستند نیز ترغیب کند. در این صورت هم، بدافزارها به سیستم شما نفوذ کرده و اطلاعات شما را جمع‌آوری می‌کنند.

به طور کلی، حملات پیام‌رسان‌ها به علت استفاده حمله‌کننده از روش‌های فریب‌دهنده در قالب پیام‌ها، به‌سادگی می‌توانند موجب تحریک شما شده و منجر به انجام اعمالی از سوی شما شوند که به ضررتان باشد و امنیت شما را به خطر بیندازد.

حملات شبکه‌های اجتماعی

حملات شبکه‌های اجتماعی یکی از رایج‌ترین انواع حملات سایبری است که در آن حمله‌کننده با استفاده از نام کاربری و رمز عبور شما، تلاش می‌کند تا به اطلاعات شما در شبکه‌های اجتماعی دسترسی پیدا کند. این حملات ممکن است با استفاده از روش‌های مختلف انجام شوند. در ادامه برخی از این موارد را برمی‌شمریم:

پیام‌های جعلی

حمله‌کننده با ارسال پیام‌های جعلی به شما، تلاش می‌کند تا شما را به ارائه اطلاعات شخصی خود درباره حساب کاربری‌تان ترغیب کند. این پیام‌ها معمولا به نام شرکت‌هایی که شما از خدمات آن‌ها استفاده می‌کنید، ارسال می‌شوند و از لحاظ ظاهری به نظر می‌رسند که از طرف آن شرکت ارسال شده‌اند.

نرم‌افزار مخرب

حمله‌کننده می‌تواند با ارسال نرم‌افزاری مخرب برای شما، تلاش کند تا به نام کاربری و رمز عبور شما دسترسی پیدا کند. این نرم‌افزارها معمولا به صورت پیام از شبکه‌های اجتماعی ارسال می‌شوند و به نظر می‌رسند که از یک منبع قابل اعتماد ارسال شده‌اند

لینک‌های جعلی

حمله‌کننده می‌تواند با ارسال لینک‌های جعلی، شما را به ورود به سایت‌های جعلی

که شبیه به سایت‌های اصلی به نظر می‌رسند، ترغیب کند. این سایت‌های جعلی معمولا به صورت بسیار مشابه با سایت‌های اصلی طراحی شده‌اند و شما را وادار به ارائه اطلاعات حساب کاربری خود در آن سایت می‌کنند.

راه‌های مقابله با حملات سایبری رایج

در این بخش به طور مشخص به راه‌های مقابله با هر یک از حملات سایبری می‌پردازیم.

راهکارهای مقابله با حملات فیشینگ

آگاهی از نوع حمله: برای مقابله با حملات فیشینگ، انواع حملات فیشینگ و روش‌های این نوع از حملات را بشناسید.

عدم اعتماد به پیام‌های ناشناس: به پیام‌های ایمیل، پیامک یا پیام‌های مستقیم در شبکه‌های اجتماعی از فرستندگان ناشناس اعتماد نکنید.

بررسی لینک‌های دریافتی: همواره تلاش کنید لینک‌های موجود در پیام‌هایی که دریافت می‌کنید را بررسی کنید و از اعتبار و امنیت آن‌ها مطمئن شوید و اگر مطمئن نشدید هرگز آن‌ها را باز نکنید.

عدم ارائه اطلاعات حساس: هرگز اطلاعات حساسی مانند نام‌کاربری، رمز عبور، شماره کارت اعتباری و غیره را در پیام‌هایی که دریافت می‌کنید، وارد نکنید.

استفاده از نرم‌افزارهای آنتی‌ویروس: استفاده از آنتی‌ویروس‌ها و بررسی منظم سیستم‌های خود برای تشخیص نرم‌افزارهای مخرب می‌تواند به شما کمک کند تا از حملات فیشینگ محافظت کنید.

گزارش حمله: در صورت دریافت پیام‌های فیشینگ، آن‌ها را همیشه و سریع گزارش

کنید تا برای دیگران هم خطری نداشته باشد.
افزایش آگاهی: آگاهی و دانش خود درباره حملات فیشینگ را بالا ببرید، تا بیشتر و بهتر از خودتان در برابر این نوع حملات محافظت کنید.

راهکارهای مقابله با حملات DDoS

استفاده از فایروال: استفاده از فایروال‌ها برای شناسایی و مسدودکردن آدرس‌های آی.پی (IP) مهاجم، می‌تواند به کاهش حملات DDoS کمک کند.
استفاده از CDN: استفاده از CDN یا شبکه توزیع محتوا، به شما کمک می‌کند تا بار ترافیک سایت خود را به سرورهای مختلف در سراسر جهان توزیع کنید. این کار می‌تواند برای شما امنیت بیش‌تری در برابر حملات DDoS فراهم کند.
استفاده از سرویس‌های حفاظت از حملات DDoS: با استفاده از سرویس‌های حفاظت از حملات DDoS می‌توانید سرعت و امنیت سایت خود را افزایش دهید.
تنظیمات سرور: تغییر تنظیمات سرور به شما کمک می‌کند تا بتوانید در برابر حملات DDoS مقاومت کنید. مثلا محدودکردن تعداد اتصالات درخواست‌های HTTP و افزایش حافظه نهان سرور.

راهکارهای مقابله با ویروس‌ها و بدافزارها

نصب یک برنامه آنتی‌ویروس معتبر: نصب یک آنتی‌ویروس معتبر می‌تواند سیستم شما را در برابر حمله ویروس‌ها و بدافزارها محافظت کند.
به‌روزرسانی مرتب نرم‌افزارها و سیستم‌عامل: به‌روزرسانی سیستم‌عامل و نرم‌افزارهای مورد استفاده شما، از لحاظ امنیتی شما را بروز نگاه می‌دارد و به معنی کاهش احتمال آسیب‌دیدن سیستم‌تان توسط بدافزارها است.
بازنکردن فایل‌های ناشناخته: بازنکردن فایل‌هایی که از منابع ناشناخته یا مشکوکی ارسال شده‌اند، می‌تواند از حملات ویروس‌ها و بدافزارها جلوگیری کند.
استفاده از فایروال: استفاده از یک فایروال می‌تواند به شما در تشخیص و جلوگیری از حملات ویروس‌ها و بدافزارها کمک کند.
آگاهی از رفتار امنیتی در اینترنت: داشتن آگاهی کافی از رفتار امنیتی در اینترنت و

همچنین آموزش خود و افراد دیگر درباره رفتارهایی که باید در برابر حملات ویروس‌ها و بدافزارها داشته باشید، می‌تواند امنیت سیستم شما را تضمین کند.

راهکارهای مقابله با حملات نفوذ

به‌روزرسانی سیستم عامل و نرم‌افزارها: بررسی و به‌روزرسانی سیستم عامل و نرم‌افزارهای مورد استفاده به صورت دوره‌ای، و به‌روزبودن آنتی‌ویروس و فایروال، کاهش آسیب‌پذیری‌های جدید را در بر خواهد داشت.

تنظیمات امنیتی سیستم: اعمال تنظیمات امنیتی مانند محدودکردن دسترسی کاربران به سیستم، رمزنگاری اطلاعات حساس، محدودکردن دسترسی به پورت‌های مشخص و سرویس‌های خاص، ایجاد سطوحی متفاوت از دسترسی‌های کاربر و مدیر، محدودکردن سطح دسترسی به فایل‌ها و سرویس‌ها و ارتقای سطح رمزنگاری از جمله تنظیماتی هستند که شانس نفوذ به سیستم شما را کاهش می‌دهند.

استفاده از فایروال: نصب و تنظیم فایروال می‌تواند به کنترل دسترسی‌ها به برنامه‌ها و خدمات شبکه کمک کند و همچنین می‌تواند ترافیک‌های غیرمجاز را تشخیص داده و مسدود کند.

رفع آسیب‌پذیری‌ها: شناسایی و رفع آسیب‌پذیری‌های موجود در سیستم و شبکه‌های مربوط به آن، می‌تواند احتمال نفوذ و دسترسی غیرمجاز به سیستم را کاهش دهد.

آموزش کاربران: آموزش کاربران درباره رفتارهای امنیتی، ارزشمند است. این آموزش می‌تواند شامل نکاتی مانند شناسایی ایمیل‌های فیشینگ، استفاده از رمز عبور قوی و تغییر دوره‌ای آن و همچنین پشتیبان‌گیری از اطلاعات باشد.

راهکارهای مقابله با حملات پیام‌رسان‌ها

به‌روزرسانی اپلیکیشن پیام‌رسان مورد استفاده: مطمئن باشید از آخرین نسخه از پیام‌رسان مورد استفاده خود استفاده می‌کنید.

رمز عبور قوی و مناسب: برای حساب‌های خود رمز عبور قوی و مناسب انتخاب کنید که احتمال حدس را برای حمله‌کننده از بین ببرید.

تایید هویت دومرحله‌ای: اغلب پیام‌رسان‌ها دارای قابلیت تایید هویت دومرحله‌ای

هستند که با فعال‌سازی آن می‌توان از حملات پیام‌رسان‌ها جلوگیری کرد. در این روش، برای ورود به حساب کاربری، علاوه بر نام کاربری و رمز عبور، یک کد امنیتی نیز به شماره تلفن همراه یا ایمیل کاربر ارسال می‌شود که با واردکردن آن، ورود به حساب کاربری امکان‌پذیر می‌شود. استفاده از این روش امنیتی کار را برای هکرها دشوار می‌کند.

عدم بازکردن پیام‌های ناشناخته: برای جلوگیری از حملات پیام‌رسانی، پیام‌های ناشناخته را باز نکنید و از دانلود فایل‌های پیوست‌شده در این پیام‌ها و کلیک روی لینک‌های ارسالی اجتناب کنید.

آگاهی از حملات پیام‌رسانی: برای مقابله با حملات پیام‌رسانی، اولین قدم آگاهی از انواع حملات پیام‌رسانی و شیوه‌های عملکرد آن‌ها است. با شناختن روش‌های حمله، می‌توانید با استفاده از راهکارهای امنیتی مناسب عملکرد خوب و امنی در قبال حفاظت از دستگاه و اطلاعات خود داشته باشید.

راهکارهای مقابله با حملات شبکه‌های اجتماعی

آگاهی از نحوه عملکرد حملات شبکه‌های اجتماعی: آگاهی از نوع حملات و روش‌هایی که حمله‌کنندگان برای دستیابی به اطلاعات شما استفاده می‌کنند، کمک می‌کند تا بتوانید در برابر حملات آن‌ها مقابله کنید.

به‌روزرسانی اپلیکیشن شبکه‌های اجتماعی مورد استفاده: همیشه مطمئن باشید که از آخرین نسخه از اپلیکیشن‌های شبکه‌های اجتماعی مورد استفاده خود استفاده می‌کنید.

استفاده از رمز عبور قوی: استفاده از رمز عبوری قوی و پیچیده که شامل حروف بزرگ و کوچک، اعداد و نشانه‌های خاص باشد، می‌تواند در برابر حملات شبکه‌های اجتماعی به خوبی از شما محافظت کند.

تایید هویت دومرحله‌ای: استفاده از تایید هویت دومرحله‌ای برای ورود به حساب کاربری شما، می‌تواند به شما کمک کند تا در برابر حملات شبکه‌های اجتماعی محافظت کنید.

اطمینان از صحت لینک‌ها: اطمینان حاصل کنید که لینک‌هایی که می‌خواهید روی آن‌ها کلیک کنید، از منابع معتبر و امن هستند.

محافظت از اطلاعات شخصی: تلاش کنید از اطلاعات شخصی خود در شبکه‌های

اجتماعی محافظت کنید و فقط اطلاعاتی را به اشتراک بگذارید که برای شما دردساز نشوند.