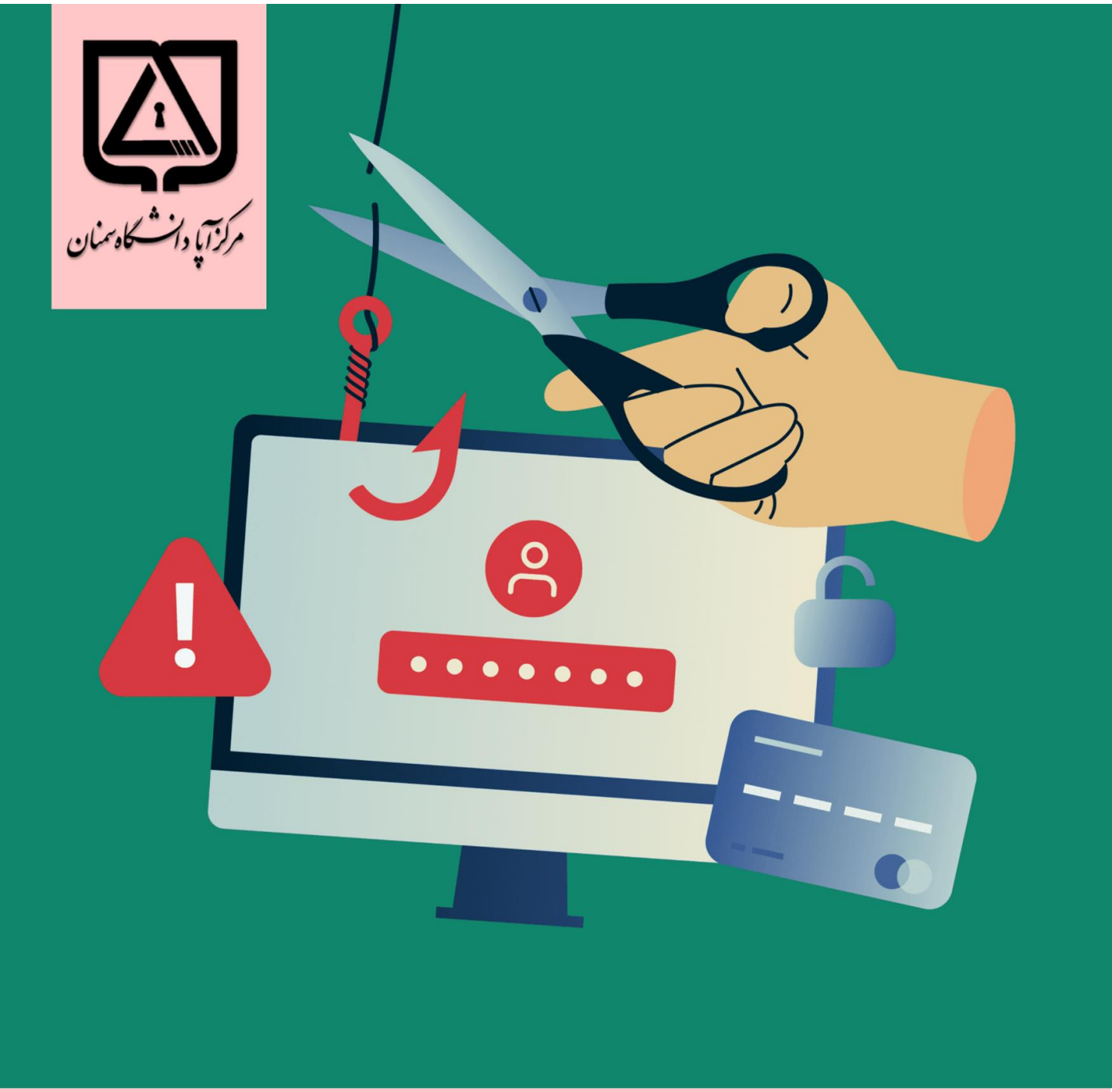
مرکز آپا دانشگاه سمنان



خبرنامه الکترونیکی ۷۷

مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

امنیت هوشمندانه در سازمان (بخش سوم)

شماره هفتاد و هفتم، سال نهم، خرداد ۱۴۰۵ | کاری از تیم تولید محتوای مرکز تخصصی آپای دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir ۰۲۳-۳۱۵۳۵۰۲۱ @semcert

فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

اخبار امنیت سایبری

کشف مجموعه آسیب‌پذیری‌های ایمنی حافظه با امکان اجرای کد دلخواه در Mozilla Thunderbird

آسیب‌پذیری‌های CVE-۲۰۲۶-۸۹۷۴ ،CVE-۲۰۲۶-۸۹۷۳ و CVE-۲۰۲۶-۸۹۷۵ با شدت ۹.۸ مجموعه‌ای از ضعف‌های مرتبط با ایمنی حافظه (Memory Safety) در نرم‌افزار Mozilla Thunderbird هستند. این مشکلات در نسخه‌های مختلف Thunderbird مشاهده شده و برخی از آن‌ها نشانه‌هایی از خرابی حافظه (Memory Corruption) را نشان می‌دهند. خرابی حافظه می‌تواند باعث شود مهاجم با ارسال داده یا محتوای مخرب، کنترل اجرای برنامه را در اختیار بگیرد. در صورت بهره‌برداری موفق، امکان اجرای کد دلخواه روی سیستم قربانی وجود دارد. این نوع ضعف‌ها معمولاً از طریق ایمیل‌های مخرب یا محتوای پردازش‌شده توسط برنامه قابل سوءاستفاده هستند. شدت این آسیب‌پذیری‌ها بالا ارزیابی می‌شود زیرا می‌توانند به اجرای کد از راه دور و تسلط مهاجم بر سیستم منجر شوند. موزیلا این مشکلات را در نسخه‌های جدید Firefox و Thunderbird برطرف کرده است. به‌روزرسانی فوری نرم‌افزار برای جلوگیری از سوءاستفاده ضروری است.

محصولات تحت تاثیر:

Thunderbird ۱۵۰

Mozilla Thunderbird ۱۴۰.۱۰

Firefox ESR ۱۱۵.۳۶

Firefox ESR ۱۴۰.۱۱

توصیه های امنیتی:

به‌روزرسانی فوری Thunderbird و Firefox ESR به نسخه‌های اصلاح‌شده:

Thunderbird ۱۵۱

Thunderbird ۱۴۰.۱۱

Firefox ۱۵۱

Firefox ESR ۱۱۵.۳۶ ،۱۴۰.۱۱

خودداری از باز کردن ایمیل‌ها یا پیوست‌های مشکوک تا زمان اعمال بروزرسانی.

فعال‌سازی قابلیت‌های امنیتی سیستم‌عامل مانند DEP، ASLR و Sandboxing.

استفاده از آنتی‌ویروس و EDR برای شناسایی رفتارهای مرتبط با Memory Corruption و RCE.

محدودسازی اجرای اسکریپت‌ها و محتوای فعال در ایمیل‌ها.

پایش مداوم سیستم برای شناسایی کرش‌ها یا رفتارهای غیرعادی در

کشف آسیب پذیری در افزونه ProSolution WP Client وردپرس

آسیب‌پذیری CVE-۲۰۲۶-۶۵۵۵ یک نقص امنیتی با درجه حیاتی (Critical) و نمره ۹.۸ از نوع آپلود فایل غیرمجاز (Arbitrary File Upload) در افزونه ProSolution WP Client (نسخه‌های ۲.۰.۰ و قبل از آن) در سیستم مدیریت محتوای وردپرس است. این نقص امنیتی به مهاجمان احراز‌هویت‌نشده و از راه دور (Unauthenticated) اجازه می‌دهد تا فایل‌های مخرب PHP خود را روی سرور آپلود کرده و به اجرای کد از راه دور (Remote Code Execution - RCE) دست یابند. ریشه این آسیب‌پذیری به یک نقص منطقی در فرآیند اعتبارسنجی آرایه‌ای از فایل‌ها (Array Validation Mismatch) برمی‌گردد. در کدهای این افزونه، مکانیسم احراز اصالت پسوند و نوع محتوا (MIME type) تنها بر روی اولین فایل موجود در آرایه آپلود اعمال می‌شود. با این حال، در گام بعدی، سیستم تمام فایل‌های موجود در آرایه را بدون اعتبارسنجی پردازش کرده و در یک دایرکتوری با دسترسی عمومی وب ذخیره می‌کند. مهاجم با سوءاستفاده از این نقص، یک فایل مجاز و سالم را به عنوان فایل اول و یک فایل مخرب (مانند Web Shell) را به عنوان فایل دوم ارسال کرده و مکانیسم امنیتی را کاملاً دور می‌زند.

محصولات تحت تاثیر:

افزونه ProSolution WP Client وردپرس، نسخه‌های ۲.۰.۰ و پیش از آن.

توصیه های امنیتی:

با توجه به اینکه این آسیب‌پذیری بدون نیاز به احراز هویت قابل بهره‌برداری بوده و مستقیماً منجر به کنترل کامل سرور (RCE) می‌شود، به مدیران سایت‌های وردپرسی توصیه می‌شود اقدامات زیر را به‌سرعت انجام دهند:

غیرفعال‌سازی یا حذف افزونه: تا زمان انتشار یک به‌روزرسانی رسمی و امن از سوی توسعه‌دهنده، پیشنهاد می‌شود این افزونه فوراً غیرفعال یا کاملاً حذف شود.

محدودسازی اجرای اسکریپت: مدیران سرور باید اجرای فایل‌های PHP را در دایرکتوری‌های مربوط به آپلود فایل (مانند wp-content/uploads) از طریق کانفیگ وب‌سرور (Nginx یا Apache) کاملاً مسدود کنند.

بررسی نشانه‌های آلودگی (IoC): دایرکتوری‌های آپلود این افزونه باید به طور دقیق برای یافتن فایل‌های PHP ناشناخته یا مشکوک که ساختاری چندگانه در درخواست آپلود داشته‌اند، اسکن و پایش شوند.

کشف آسیب پذیری در Nginx

یک آسیب‌پذیری Zero-Day با نام nginx-poolslip در NGINX شناسایی شده است که امکان اجرای کد از راه دور (RCE) را فراهم می‌کند. این آسیب‌پذیری توسط تیم امنیتی NebSec و پژوهشگری با نام Vega افشا شده و تاکنون شناسه CVE رسمی و وصله امنیتی رسمی برای آن منتشر نشده است.

این نقص، مکانیزم داخلی مدیریت حافظه Memory Pool Handling (NGINX) را هدف قرار می‌دهد و به‌عنوان یک ASLR Bypass شناخته می‌شود. مهاجم می‌تواند بدون نیاز به احراز هویت و تنها از طریق ارسال درخواست‌های crafted شده، کنترل اجرای کد را در سرور هدف به دست آورد. طبق گزارش منتشرشده، این آسیب‌پذیری ادامه‌ای از حملات مرتبط با نقص قبلی موسوم به nginx-rift و همچنین CVE-۲۰۲۶-۴۲۹۴۵ محسوب می‌شود.

این آسیب‌پذیری هنوز دارای شناسه CVE و بردار رسمی CVSS نیست، اما بر اساس اطلاعات منتشرشده، امکان بهره‌برداری از راه دور و بدون نیاز به احراز هویت وجود دارد. نقص در مدیریت Memory Pool‌های داخلی NGINX باعث می‌شود مهاجم بتواند از طریق درخواست‌های HTTP دستکاری‌شده، فرآیندهای Worker را دچار فساد حافظه (MemoryCorruption) کند. پژوهش NebSec نشان می‌دهد که مهاجم می‌تواند مکانیزم امنیتی ASLR را دور زده و شرایط لازم برای اجرای کد دلخواه روی سرور را فراهم کند. این موضوع می‌تواند منجر به تصاحب کامل سرور، اجرای کد، اختلال سرویس و دسترسی به داده‌های حساس شود.

محصولات تحت‌تأثیر:

NGINX ۱.۳۱.۰

توصیه های امنیتی:

برای رفع این آسیب‌پذیری و جلوگیری از سوءاستفاده مهاجمان، اقدامات زیر ضروری است:

اطلاعیه‌های امنیتی F۵ و NGINX را به‌صورت مستمر بررسی شود.

دسترسی مستقیم به Interface‌های مدیریتی و سرویس‌های حساس محدود شود.

NUVATION ENERGY

کشف آسیب پذیری در Nuvation Energy MSC

MSC(Nuvation Energy Multi-Stack Controller) یک مؤلفه/کنترلر در سامانه‌های ذخیره‌سازی انرژی و مدیریت پشته های باتری است که معمولاً در محیط‌های عملیاتی و صنعتی استفاده می‌شود.

اخیراً یک آسیب‌پذیری بحرانی با شناسه CVE-۲۰۲۵-۶۴۱۲۱ و امتیاز ۱۰.۰ :CVSS v۴.۰ برای این محصول ثبت شده است. این آسیب‌پذیری از نوع CWE-۲۸۸(Authentication Bypass Using an Alternate Path or Channel) بوده و در صورت بهره‌برداری موفق، مهاجم می‌تواند بدون احراز هویت سازوکارهای ورود را دور بزند.

محصولات تحت تاثیر:

MSC(Nuvation Energy Multi-Stack Controller)

بازه نسخه‌های آسیب‌پذیر: از ۲.۳.۸ تا قبل از ۲.۵.۱

طبق Advisory دراگوس، این آسیب‌پذیری در Platform ۲.۳.۸ معرفی و در Platform ۲.۵.۱ رفع شده است.

توصیه های امنیتی:

به‌روزرسانی فوری: ارتقاء MSC به ۲۲.۴.۰ / nPlatform ۲.۵.۱ (یا نسخه‌های جدیدتر در صورت ارائه).

کاهش سطح در معرض بودن تا زمان ارتقا: دسترسی به MSC را از شبکه‌های غیرقابل‌اعتماد/خصمانه محدود کنید (تفکیک شبکه، VPN، Allowlist) و سرویس‌های مدیریتی را فقط از مسیرهای مجاز در دسترس قرار دهید.

سخت‌سازی تنظیمات: طبق توصیه Dragos، احراز هویت MSC را فعال کرده و رمز عبور قوی تنظیم کنید.

کاهش ریسک جانبی (اختیاری): در صورت عدم نیاز عملیاتی، دسترسی به سرویس nCloud را محدود کنید.

مرکز آپا دانشگاه سمنان

امنیت هوشمندانه در سازمان

امنیت هوشمندانه در سازمان (بخش سوم)

تشخیص ایمیل‌ها، پیام‌ها و لینک‌های جعلی - مهارتی ضروری برای هر کارمند

در بخش‌های قبلی درباره تهدیدات رایج و سپس مدیریت رمزهای عبور صحبت کردیم.
اما یکی از خطرناک‌ترین و در عین حال رایج‌ترین روش‌های حمله، فیشینگ و پیام‌های جعلی است؛ پیام هایی که وانمود می‌کنند قانونی‌اند، اما هدفشان سرقت اطلاعات یا آلوده کردن سیستم شماست.
در این بخش یاد می‌گیریم چگونه تنها با چند نشانه ساده، ۴۰ تا ۷۰ درصد پیام‌های جعلی را در همان نگاه اول تشخیص دهیم.

۱. فیشینگ چیست و چرا خطرناک است؟

فیشینگ به مجموعه‌ای از حملات گفته می‌شود که در آن مهاجم تلاش می‌کند شما را فریب دهد تا:

- رمز عبور خود را وارد کنید
- اطلاعات شخصی یا سازمانی ارائه دهید
- روی لینک آلوده کلیک کنید
- فایل مخرب را باز کنید

این حملات معمولاً وانمود می‌کنند از طرف:

- واحد مالی
- واحد منابع انسانی
- بانک
- سامانه‌های ثبت‌نام، تسویه حساب یا حقوق
- همکاران
- یا حتی مدیر سازمان

ارسال شده‌اند.
چون پیام ظاهراً «عادی» است، قربانی معمولاً بدون مکث آن را باز می‌کند.

۲. پنج نشانه طلایی یک پیام یا ایمیل مشکوک

۲-۱. پیام‌های عجیب با «فوریت غیرعادی»

جملاتی مثل:

- همین الان کلیک کنید
- حساب شما مسدود می‌شود
- تا ۲ ساعت آینده اقدام کنید
- برای دریافت حقوق باید فرم جدید را پر کنید

مهاجمان از ترس و عجله سوءاستفاده می‌کنند

۲-۲. غلط‌های نگارشی و ادبی

در بسیاری از ایمیل‌های جعلی:

- لحن رسمی با جملات عجیب ترکیب می‌شود
- شکل نگارش واحد، طبیعی نیست
- نام‌ها یا اصطلاحات سازمان اشتباه است

نمونه:

«کاربر گرامی، لطفن جهت بروزرصانی پروفایل کلیک فرمایید»

۲-۳. آدرس فرستنده واقعی نیست

مثال:

به‌جای:

info@semnan.ac.ir

ممکن است چنین باشد:

info-semnan@secure-mail.co

یا:

semn۴n-support@tech-service.com

ظاهر آدرس شبیه است ولی کاملاً متفاوت.

۲-۴. لینک‌ها پشت متن پنهان شده‌اند

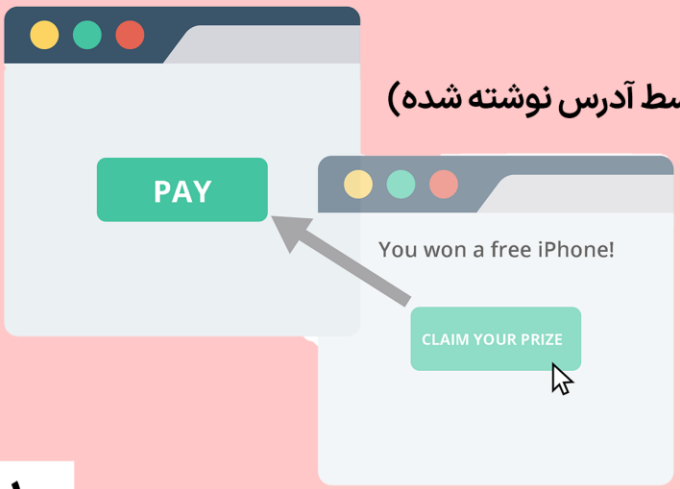
متنی مانند «ورود به سامانه» ممکن است به سایتی نامعتبر هدایت کند.

برای بررسی، روی لینک حمله نکنید؛

بلکه ماوس را روی لینک نگه دارید تا آدرس واقعی را ببینید.

اگر این‌ها را دیدید، خطر جدی است:

- آدرس با http شروع می‌شود، نه https
- آدرس دامنه عجیب است یا شباهت جعلی دارد
- نام برند در ابتدای دامنه نیست (مثلاً یاهو در وسط آدرس نوشته شده)



۵-۲. فایل‌های ضمیمه ناشناس یا غیرمرتبط

فایل‌هایی با پسوندهای:

- .exe
- .zip
- .jar
- .xlsm
- .scr

در ایمیل‌های رسمی تقریباً هیچ‌وقت ارسال نمی‌شود.

حتی فایل Word یا Excel هم می‌تواند آلوده باشد.

۳. چه پیام‌هایی بیشترین قربانی را در سازمان‌ها می‌گیرند؟

براساس تجربه آپاها و مراکز CERT، بیشترین موارد فریب مربوط به پیام‌هایی با موضوعات:

- «مشاهده فیش حقوقی جدید»
- «رسید پرداخت»
- «بروزرسانی حساب کاربری»
- «تغییر رمز اجباری»
- «نتایج ارزیابی عملکرد»
- «درخواست فوری مدیر»
- «فاکتور تسویه»
- «احراز هویت مجدد سامانه»

این پیام‌ها برای کارکنان بسیار آشنا هستند، به همین دلیل امنیت‌شان نادیده گرفته می‌شود.

۴. چک‌لیست ۱۰ ثانیه‌ای تشخیص پیام جعلی

این چک‌لیست برای روی میز کار عالی است:

۱. آیا پیام غیرمنتظره است؟
۲. آیا لحن پیام عجیب یا بیش از حد فوری است؟
۳. آیا آدرس فرستنده واقعی نیست یا تفاوت جزئی دارد؟
۴. آیا لینک، دامنه ناشناسی است؟
۵. آیا غلط املایی یا نگارشی دارد؟
۶. آیا پیوست غیرعادی دارد؟
۷. آیا درخواست اطلاعات حساس دارد؟
۸. آیا شما را تهدید یا عجله می‌اندازد؟
۹. آیا پیام به چند نفر دیگر هم ارسال شده؟
۱۰. آیا منبع پیام را می‌توانید تلفنی از داخل سازمان تأیید کنید؟

اگر حتی یکی از این موارد برقرار باشد؛ باز نکنید و گزارش دهید.

۵. نمونه واقعی یک ایمیل جعلی (بازنویسی‌شده)

موضوع: «فیش حقوقی مرداد - نسخه جدید»

فرستنده: hr@semnan-payment.com

متن:

«کاربر گرامی،

برای دریافت فیش حقوق مرداد لطفن تا ۶ ساعت آینده فایل پیوست را دانلود کرده و رمز دریافتی را وارد کنید.

عدم اقدام موجب عدم پرداخت می‌شود.»

نشانه‌ها:

- دامنه جعلی
- غلط نگارشی
- فوریت ساختگی
- فایل ZIP

این الگو بارها در سازمان‌های مختلف مشاهده شده است.

۶. اگر روی لینک جعلی کلیک کردیم چه کنیم؟

مهم:

این اشتباه برای هر کارمندی ممکن است اتفاق بیفتد.

مهم این است که سریع و درست عمل کنید.

اول: پنجره را ببندید، اطلاعات وارد نکنید.

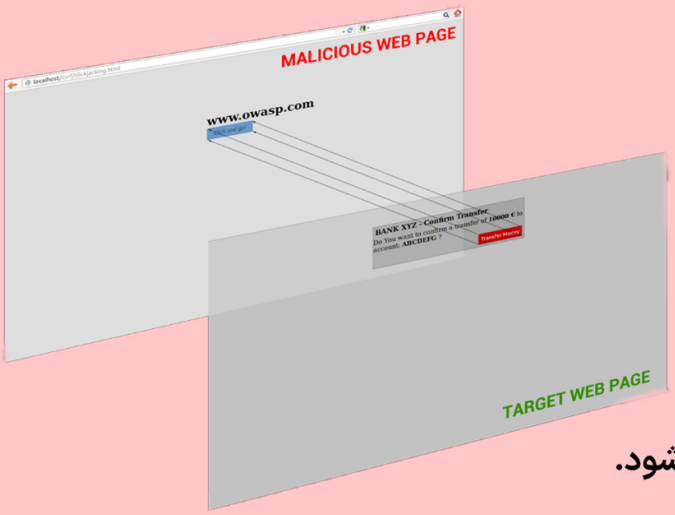
دوم: فوراً رمزهای مرتبط را تغییر دهید.

سوم: موضوع را به واحد IT گزارش کنید.

چهارم: مرورگر را ببندید و سیستم را ری‌استارت کنید.

پنجم: اگر فایل دانلود شده، آن را باز نکنید.

گزارش سریع باعث جلوگیری از خسارت‌های بزرگ می‌شود.



امنیت هوشمندانه در سازمان (بخش سوم)

۷. چگونه ایمن پاسخ دهیم؟

برای برخورد امن با پیام‌های مشکوک تنها کافی است:

- روی لینک‌ها کلیک نکنید
- فایل‌ها را باز نکنید
- پاسخ ندهید
- پیام را فوراً به واحد IT یا مرکز آپای سازمان ارسال کنید
- از طریق تلفن داخلی، صحت پیام را از ارسال‌کننده احتمالی بررسی کنید

این رفتار ساده، صدها حادثه را پیش از وقوع متوقف می‌کند.

۸. جمع‌بندی بخش سوم

در این شماره یاد گرفتیم:

- پیام‌ها و لینک‌های جعلی چگونه کار می‌کنند
- مهاجمان چگونه از ترس یا عجله سوءاستفاده می‌کنند
- پنج نشانه طلایی برای تشخیص پیام مشکوک چیست
- چک‌لیست سریع ۱۰ ثانیه‌ای چگونه جلوی اشتباه را می‌گیرد
- و اگر اشتباهی روی لینک کلیک کردیم، چه کاری باید انجام دهیم

در بخش چهارم مجموعه:

امنیت تجهیزات کاری (موبایل، لپ‌تاپ، فلش، شبکه وای‌فای) و نقش هر کارمند در حفاظت از دستگاه ها را بررسی خواهیم کرد.

ما را در سایت زیر دنبال کنید :

https://cert.semnan.ac.ir