سازمان پدافند غیرعامل کشور

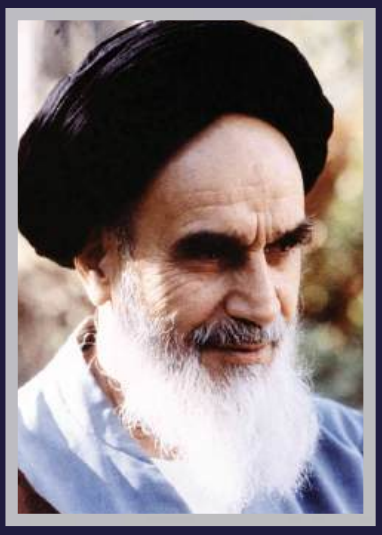
پدافند سایبری

کتابچه آموزش عمومی

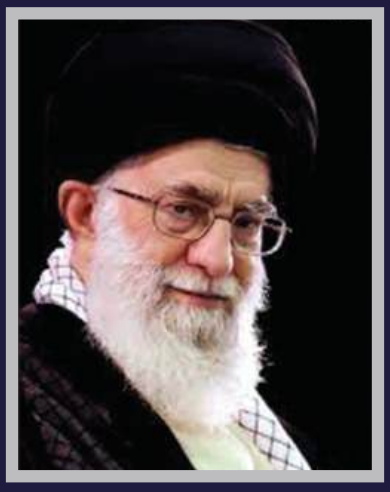
سازمان پدافند غیرعامل کشور




تابستان ۱۴۰۴



هر انسان مخلص و متعهدی که آمادگی دفاع لازم را لازمه حیات جامعه اسلامی بداند در نزد خدا آبرو پیدا می کند.



پدافند غیرعامل مثل مصونیت سازی بدن انسان است، از درون مارا مصون می‌کند. معنایش این است ولو دشمن تهاجمی بکند و زحمتی هم بکشد و ضرب و زوری هم بزند اثری نخواهد کرد. پدافند غیرعامل نتیجه اش این است.

"درمقابل شیوه های پیچیده تهاجم دشمنان، پدافند غیرعامل باید کاملا هشیار و جدی باشد."

فهرست مطالب

وَ أَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَ مِنْ رِباطِ الْخَيلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَ عَدُوَّكُمْ وَ آخَرِينَ مِنْ دُونِهِمْ لا تَعْلَمُونَهُمُ اللَّهُ يعْلَمُهُمْ وَ ما تُنْفِقُوا مِنْ شَيءٍ فِي سَبِيلِ اللَّهِ يوَفَّ إِلَيكمْ وَ أَنْتُمْ لا تُظْلَمُون

در برابر آنها (دشمنان) آنچه توانایی دارید از "نیرو" آماده سازید (و همچنین) اسبهای ورزیده (برای میدان نبرد) تا به وسیله آن دشمن خدا و دشمن خویش را بترسانید و (همچنین) گروه دیگری غیر از اینها را که شما نمی‌شناسید و خدا می‌شناسد و هر چه در راه خدا (و تقویت بنیه دفاعی اسلام) انفاق کنید، به شما باز گردانده میشود و به شما ستم نخواهد شد.

آیه ۶۰ سوره انفال

فصل اول

مقدمه

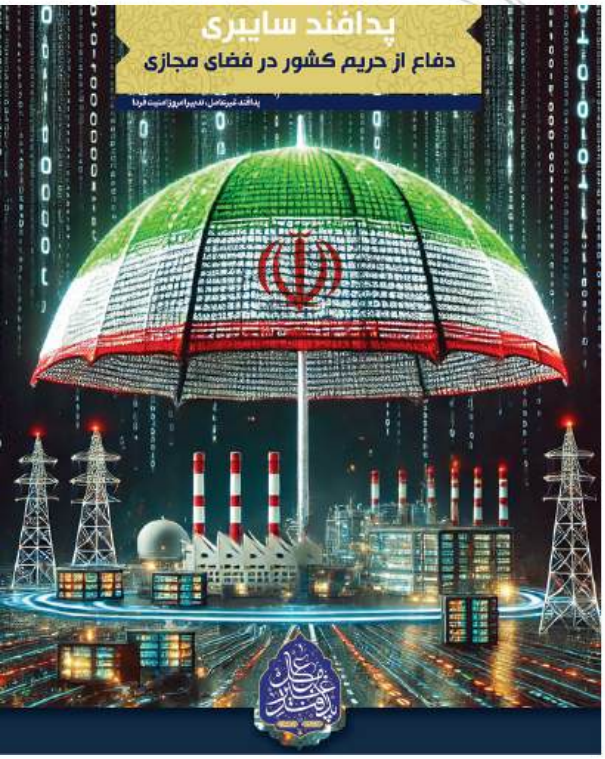
پدافند سایبری به معنای استفاده از روش‌های غیرنظامی، پیشگیرانه و حفاظتی در برابر تهدیدات فضای سایبری است.

مقدمه

پدافند سایبری چیست؟

در عصر حاضر، فناوری اطلاعات و ارتباطات به جزئی جدایی‌ناپذیر از زندگی بشر تبدیل شده است؛ اما همزمان با افزایش وابستگی جوامع به زیرساخت های دیجیتال، تهدیدات سایبری نیز رشد فزاینده‌ای یافته‌اند. حملات سایبری نه تنها نهادها و سازمان‌های حیاتی را هدف قرار می‌دهند، بلکه شهروندان عادی را نیز در معرض خطراتی همچون سرقت اطلاعات شخصی، فریب های اینترنتی، قطع خدمات عمومی و حتی خسارات مالی قرار می‌دهند. در این میان، نقش مردم در آمادگی و واکنش هوشمندانه به تهدیدات سایبری، همانند پدافند غیرعامل در برابر تهدیدات نظامی، نقشی اساسی است.

پدافند سایبری به معنای استفاده از روش‌های غیرنظامی، پیشگیرانه و حفاظتی در برابر تهدیدات فضای سایبری است. این مفهوم با هدف ارتقای تاب‌آوری ملی در برابر جنگ های نوین (که اغلب ترکیبی از عملیات سایبری، روانی و زیرساختی هستند) شکل گرفته است. بر اساس اسناد بالادستی از جمله ماده ۵۸ قانون احکام دائمی برنامه‌های توسعه و سیاست‌های کلی نظام، آموزش عمومی مردم در زمینه پدافند غیرعامل، یک تکلیف حاکمیتی تلقی می‌شود. با این حال، بررسی های میدانی در بحران‌های اخیر (مانند جنگ ۱۲ روزه) نشان می دهد که سطح آگاهی عمومی مردم در خصوص تهدیدات سایبری پایین است و این مسئله منجر به آسیب پذیری شده است.



هدف این کتابچه، ارائه آموزش‌های کاربردی، ساده و قابل‌اجرا برای عموم مردم است تا بتوانند پیش، حین و پس از وقوع بحران های سایبری، رفتار مناسب و ایمن از خود نشان دهند. این راهنما در شش بخش تهیه شده که در ادامه به تفصیل ارائه می‌گردد و سعی شده تا زبان آن ساده، غیرتخصصی و برگرفته از تجربیات واقعی و مستند باشد.

فصل دوم

سناریوهای اصلی تهدید سایبری و دستورات آمادگی عمومی

در این بخش، به رایج‌ترین سناریوهای تهدیدات سایبری پرداخته می‌شود که ممکن است زندگی روزمره افراد جامعه را تحت تأثیر قرار دهند؛ همچنین آموزش های آمادگی عمومی درمورد هر سناریو توضیح داده خواهد شد.

سناریوهای اصلی تهدید سایبری

رایج ترین تهدیدات سایبری

در دنیای امروز که ارتباطات دیجیتال بخشی جدانشدنی از زندگی روزمره شده، تهدیدات سایبری نیز با سرعت فزاینده‌ای گسترش یافته‌اند. آگاهی از این تهدیدها و درک نحوه عملکرد آن‌ها، نخستین گام در مسیر پدافند مؤثر سایبری است. در این بخش به رایج‌ترین سناریوهای تهدید سایبری پرداخته می‌شود که عموم مردم به‌صورت مستقیم یا غیرمستقیم با آن‌ها مواجه می‌شوند.

رایج ترین تهدیدات سایبری در جامعه امروزی ما موارد زیر می باشد:

- فیشینگ
- مهندسی اجتماعی
- باج‌افزارها
- حملات به وای‌فای عمومی
- نفوذ به خانه‌های هوشمند
- شبکه‌های اجتماعی و کلاهبرداری‌های آنلاین

۲-۱. فیشینگ (Phishing)

فیشینگ یکی از رایج‌ترین روش‌های کلاهبرداری سایبری است که در آن مهاجم با جعل هویت یک فرد یا سازمان معتبر (مانند بانک، شرکت خدماتی یا حتی یک دوست)، تلاش می‌کند کاربر را فریب دهد تا اطلاعات حساس خود را در اختیار او قرار دهد. این اطلاعات می‌تواند شامل رمز عبور، کد تأیید پیامکی، شماره کارت بانکی یا سایر داده های شخصی باشد.

شیوه‌های متداول فیشینگ:

ایمیل‌های جعلی:
پیام‌هایی که ظاهراً از طرف بانک، سازمان دولتی یا فروشگاه اینترنتی معتبر ارسال شده‌اند، اما در واقع از آدرس‌های تقلبی می آیند.
این ایمیل‌ها معمولاً حاوی لینک‌هایی هستند که به وب‌سایت‌های جعلی هدایت می‌شوند و ظاهر آن‌ها کاملاً شبیه سایت اصلی است.

فیشینگ پیامکی (Smishing):
ارسال پیامک‌هایی با مضمون «برداشت غیرمجاز از حساب»، «بسته اینترنت رایگان» یا «پرداخت قبض» که کاربر را به کلیک روی لینک آلوده ترغیب می‌کند.

فیشینگ صوتی (Vishing):
تماس تلفنی از سوی فردی که خود را کارمند بانک یا یک نهاد رسمی معرفی می‌کند و با ایجاد حس اضطرار (مثلاً مسدود شدن حساب بانکی)، از قربانی اطلاعات حساس را دریافت می‌کند.

نشانه‌های اصلی یک حمله فیشینگ:

- **آدرس اینترنتی مشکوک:** لینک‌هایی که حاوی غلط املایی یا دامنه‌های ناشناس هستند (مثلاً bank-ir.com به جای bank.ir).
- **درخواست اطلاعات محرمانه:** بانک‌ها و سازمان‌های معتبر هرگز از طریق ایمیل یا پیامک، رمز عبور یا اطلاعات کارت بانکی را درخواست نمی‌کنند.
- **ایجاد حس اضطرار یا ترس:** پیام‌هایی که تأکید می‌کنند «بلافاصله اقدام کنید» یا «در غیر این صورت حسابتان مسدود می شود».
- **پیشنهادهای غیرواقعی:** وعده برنده شدن جایزه یا دریافت هدیه رایگان بدون دلیل منطقی.

راهکارهای پیشگیری:

- همیشه آدرس سایت را در مرورگر خود تایپ کنید و روی لینک‌های مشکوک کلیک نکنید.
- پیش از وارد کردن اطلاعات، از وجود پروتکل امن HTTPS در آدرس سایت اطمینان حاصل کنید.
- پیام‌ها یا ایمیل‌های ناشناس را حتی برای آزمایش هم باز نکنید.
- نرم‌افزار ضدویروس معتبر نصب و به‌روزرسانی کنید.

۲-۲. مهندسی اجتماعی (Social Engineering)

مهندسی اجتماعی مجموعه‌ای از تکنیک‌ها و روش‌هاست که مهاجمان برای دستکاری رفتار و احساسات افراد به کار می‌برند تا آن‌ها را وادار کنند اطلاعات حساس را افشا کرده یا اقداماتی انجام دهند که امنیت آن‌ها را به خطر می‌اندازد. برخلاف فیشینگ که بیشتر مبتنی بر ابزارهای دیجیتال است، مهندسی اجتماعی می‌تواند هم در فضای مجازی و هم در دنیای واقعی رخ دهد.

تکنیک‌های رایج مهندسی اجتماعی:

پیش‌داوری (Pretexting):

مهاجم با ایجاد یک سناریوی ساختگی و معتبر، اعتماد قربانی را جلب می‌کند. مثلاً فردی خود را مأمور اداره برق معرفی می‌کند تا به خانه یا محل کار دسترسی پیدا کند.

طعمه‌گذاری (Baiting):

ارائه یک چیز جذاب یا رایگان (مثل یک فلش مموری، دانلود فیلم یا نرم‌افزار رایگان) برای ترغیب قربانی به استفاده از آن، که معمولاً آلوده به بدافزار است.

دنباله‌روی (Tailgating):

ورود به یک مکان حفاظت‌شده با دنبال کردن فرد مجاز، مثلاً وارد شدن به ساختمان اداری با شخصی که کارت عبور دارد.

جعل هویت (Impersonation):

وانمود کردن به این‌که شخصی شناخته‌شده یا دارای مقام رسمی است (مانند همکار، رئیس یا کارمند بانک) تا قربانی را فریب دهد.

نمونه‌های واقعی مهندسی اجتماعی:

فردی با لباس فرم پستچی وارد شرکت می‌شود و از کارمندان درخواست می‌کند برای «ارسال بسته فوری» از رایانه آن‌ها استفاده کند.

تماس تلفنی با والدین یک دانش‌آموز و ادعای اینکه فرزندشان در بیمارستان بستری شده است تا از این طریق اطلاعات یا پول دریافت شود.

نشانه‌های هشداردهنده:

- درخواست‌های غیرعادی یا خارج از روال کاری از سوی افراد ظاهراً معتبر.
- اصرار بر اقدام فوری و بدون بررسی.
- ارائه اطلاعات ناقص یا غیرقابل‌تأیید توسط فرد درخواست‌کننده.

راهکارهای پیشگیری:

- هرگز بر اساس ظاهر یا لحن دوستانه به کسی اعتماد نکنید، حتی اگر به‌نظر معتبر می‌رسد.
- اطلاعات شخصی را فقط در صورت اطمینان از هویت طرف مقابل ارائه دهید.
- در محیط‌های کاری، از ورود افراد ناشناس به مناطق حساس جلوگیری کنید.
- در فضای آنلاین، هویت افراد را از طریق کانال‌های رسمی تأیید کنید.

۲-۳. باج‌افزار و بدافزار

بدافزار (Malware) به هر نوع نرم‌افزار مخربی گفته می‌شود که برای آسیب رساندن به دستگاه‌ها، سرقت یا تغییر اطلاعات، یا ایجاد اختلال در عملکرد سیستم طراحی شده است.

باج‌افزار (Ransomware) نوعی خاص از بدافزار است که پس از آلوده کردن سیستم، فایل‌ها را رمزگذاری می‌کند و در ازای بازگرداندن دسترسی، از قربانی درخواست پرداخت پول (معمولاً به ارز دیجیتال) می‌کند.

روش‌های انتشار

۱. پیوست‌های آلوده در ایمیل‌ها

- فایل‌های Word، Excel یا PDF که حاوی ماکروهای مخرب هستند.

نمونه: ایمیل جعلی با موضوع «فاکتور پرداخت نشده» که کاربر را به باز کردن فایل ضمیمه ترغیب می‌کند.

۲. وب‌سایت‌ها و تبلیغات آلوده (Malvertising)

- بازدید از سایت‌های هک‌شده یا کلیک روی بنرهای تبلیغاتی که بدافزار را دانلود می‌کنند.

۳. حملات از طریق USB یا حافظه خارجی

- فلش مموری آلوده که با اتصال به سیستم، بدافزار را خودکار اجرا می‌کند.

۴. دانلود نرم‌افزار از منابع نامعتبر

- نسخه‌های کرک شده برنامه‌ها که حاوی کدهای مخرب هستند.

۵. آسیب‌پذیری‌های سیستم و نرم‌افزار

- استفاده از حفره‌های امنیتی در سیستم عامل یا نرم افزارهایی که به‌روزرسانی نشده‌اند.

نمونه‌های واقعی

- WannaCry (۲۰۱۷): یک باج‌افزار که با سوءاستفاده از آسیب‌پذیری ویندوز در کمتر از یک روز بیش از ۲۳۰ هزار کامپیوتر در ۱۵۰ کشور را آلوده کرد.
- NotPetya (۲۰۱۷): ابتدا به عنوان باج‌افزار معرفی شد اما هدف اصلی آن تخریب داده‌ها و اختلال در زیرساخت های حیاتی بود.
- Locky و CryptoLocker: از طریق ایمیل‌های فیشینگ منتشر می‌شدند و هزاران کاربر را مجبور به پرداخت باج کردند.

نشانه‌های آلودگی

- کند شدن ناگهانی سیستم بدون دلیل مشخص.
- تغییر نام و پسوند فایل‌ها (مثلاً file.doc به file.doc.locked).
- پیام‌های پاپ‌آپ یا صفحه قفل که از شما درخواست پرداخت پول می‌کنند.
- اختلال در اتصال به اینترنت یا عدم دسترسی به برخی وب‌سایت‌ها.
- فعالیت غیرعادی هارد دیسک حتی در حالت بیکار بودن سیستم.

پیامدهای آلودگی

- از دست رفتن دائمی داده‌های مهم در صورت نداشتن نسخه پشتیبان.
- خسارت مالی ناشی از پرداخت باج یا هزینه‌های بازیابی اطلاعات.
- افشای اطلاعات محرمانه و آسیب به اعتبار فرد یا سازمان.
- اختلال در فعالیت‌های روزمره یا کسب‌وکار.

راهکارهای پیشگیری

۱. به‌روزرسانی مداوم سیستم‌عامل و نرم‌افزارها
- نصب آخرین وصله‌های امنیتی برای بستن آسیب پذیری‌ها.

۲. استفاده از آنتی‌ویروس و ضدباج‌افزار معتبر
- فعال‌سازی قابلیت محافظت بلادرنگ (Real-time Protection).

۳. پشتیبان‌گیری منظم از اطلاعات
- نگهداری نسخه پشتیبان در حافظه خارجی یا سرویس ابری امن که به‌طور دائم به سیستم متصل نیست.

۴. احتیاط در باز کردن ایمیل‌ها و پیوست‌ها
- حتی اگر ایمیل از سوی فرد آشنا باشد، محتوای آن را بررسی کنید.

۵. محدود کردن سطح دسترسی کاربران
- استفاده از حساب‌های کاربری با سطح دسترسی محدود به جای حساب مدیر (Admin).

۶. آموزش و آگاهی‌بخشی به کاربران
- شناسایی پیام‌های مشکوک، لینک‌های آلوده و رفتار ایمن در اینترنت.

اقدامات در صورت آلودگی

- قطع فوری اتصال به اینترنت برای جلوگیری از گسترش آلودگی.
- خاموش نکردن سیستم (در برخی باج‌افزارها، خاموش کردن می‌تواند فرآیند رمزگذاری را کامل کند).
- گزارش حادثه به تیم امنیتی سازمان یا مراجع ذی صلاح (مانند پلیس فتا).
- بررسی ابزارهای رمزگشایی رایگان در وب‌سایت هایی مانند NoMoreRansom.org قبل از پرداخت باج.
- بازیابی از نسخه پشتیبان سالم در صورت وجود.

۲-۴. وای‌فای عمومی و حملات شبکه‌ای

وای‌فای عمومی به شبکه‌های بی‌سیمی گفته می‌شود که در مکان‌های عمومی مانند کافی‌شاپ‌ها، فرودگاه‌ها، هتل‌ها، کتابخانه‌ها و مراکز خرید در دسترس همگان قرار دارند. این شبکه‌ها معمولاً بدون رمز عبور یا با رمز مشترک برای همه کاربران ارائه می‌شوند.

هرچند این سرویس‌ها راحتی و دسترسی آسان به اینترنت را فراهم می‌کنند، اما به دلیل ضعف در امنیت، به یکی از نقاط اصلی حمله مجرمان سایبری تبدیل شده‌اند.

تهدیدات رایج در وای‌فای عمومی

۱. شنود داده‌ها (Packet Sniffing)

• مهاجمان می‌توانند با استفاده از ابزارهای تخصصی، داده‌های ارسالی و دریافتی شما را رهگیری کنند. این داده ها می‌توانند شامل رمز عبور، اطلاعات کارت بانکی، پیام‌ها و ایمیل‌ها باشند.

۲. حملات مرد میانی (Man-in-the-Middle)

• در این روش، مهاجم بین شما و سرور اصلی قرار می گیرد و تمام اطلاعات رد و بدل شده را مشاهده یا حتی تغییر می‌دهد. برای مثال، ممکن است آدرس بانکی را به صفحه ای جعلی هدایت کند.

۳. شبکه‌های جعلی (Evil Twin)

• مهاجم شبکه‌ای با نام مشابه وای‌فای واقعی ایجاد می کند. کاربر ناآگاه به این شبکه متصل می‌شود و تمام داده های او تحت کنترل مهاجم قرار می‌گیرد.

۴. نفوذ مستقیم به دستگاه‌ها

• برخی وای‌فای‌های عمومی اجازه برقراری ارتباط مستقیم بین دستگاه‌ها را می‌دهند. این موضوع به هکرها امکان می‌دهد تا بدون نیاز به سرور واسط، مستقیماً به دستگاه شما نفوذ کنند.

۵. بدافزار از طریق شبکه

• هکرها می‌توانند از طریق نقاط ضعف شبکه یا سیستم عامل، بدافزارهایی را به دستگاه‌های متصل ارسال کنند.

نشانه‌های خطر در وای‌فای عمومی

• شبکه‌ای که نامی مشابه با وای‌فای رسمی مکان دارد اما رمز عبور متفاوتی می‌طلبد.

• درخواست ورود به صفحات ورود (Login Pages) غیرمعمول که اطلاعات اضافی از شما می‌خواهد.

• قطع و وصل مکرر اتصال یا کندی غیرعادی سرعت.

• نمایش هشدار امنیتی مرورگر هنگام ورود به وب‌سایت ها (مثلاً «اتصال شما امن نیست»).

توصیه‌های امنیتی هنگام استفاده از وای‌فای عمومی

۱. استفاده از VPN

• یک شبکه خصوصی مجازی (VPN) تمام داده‌های شما را رمزگذاری می‌کند و مانع شنود می‌شود.

۲. فعال‌سازی فایروال

• فایروال مانع از برقراری ارتباط‌های غیرمجاز به دستگاه شما می‌شود.

۳. غیرفعال کردن اتصال خودکار به شبکه‌ها

• در تنظیمات دستگاه، قابلیت اتصال خودکار را خاموش کنید تا به شبکه‌های جعلی وصل نشوید.

۴. عدم انجام فعالیت‌های حساس

• در وای‌فای عمومی از وارد شدن به حساب‌های بانکی یا انجام خریدهای آنلاین خودداری کنید.

۵. استفاده از HTTPS

• مطمئن شوید آدرس وب‌سایت‌ها با «https://» شروع می‌شود تا ارتباط شما رمزگذاری‌شده باشد.

۶. به‌روزرسانی سیستم و برنامه‌ها

• با نصب آخرین وصله‌های امنیتی، آسیب‌پذیری‌ها کاهش می‌یابد.

۷. غیرفعال کردن اشتراک‌گذاری فایل و پرینتر

• این قابلیت‌ها در وای‌فای عمومی مسیرهای نفوذ آسان برای مهاجمان هستند.

اقدامات پس از شناسایی تهدید

• قطع فوری اتصال از شبکه مشکوک.

• تغییر رمز عبور حساب‌های مهم در اولین فرصت.

• اسکن کامل دستگاه با آنتی‌ویروس به‌روز.

• گزارش موضوع به مدیریت مکان یا مراجع ذی‌صلاح.

۲-۵. نفوذ به گوشی‌های هوشمند

گوشی‌های هوشمند امروزه به‌عنوان یکی از اصلی‌ترین ابزارهای ارتباطی و کاری، حجم عظیمی از اطلاعات شخصی، مالی و حرفه‌ای را در خود ذخیره می‌کنند. این دستگاه‌ها به دلیل اتصال دائم به اینترنت، استفاده گسترده از اپلیکیشن ها، و تبادل داده با سایر تجهیزات، هدف جذابی برای مجرمان سایبری هستند. نفوذ به گوشی هوشمند می‌تواند منجر به سرقت اطلاعات، جاسوسی، شنود مکالمات و حتی سوءاستفاده مالی شود.

روش‌های رایج نفوذ

۱. نصب اپلیکیشن‌های مخرب

- اپلیکیشن‌هایی که ظاهراً کاربردی یا سرگرم‌کننده هستند اما در پس‌زمینه، اطلاعات کاربر را جمع‌آوری و ارسال می‌کنند.

نمونه: اپلیکیشن چراغ‌قوه که دسترسی به پیامک‌ها و لیست تماس‌ها را درخواست می‌کند.

۲. اعطای مجوزهای بیش از حد به برنامه‌ها

- کاربر بدون بررسی، اجازه دسترسی به دوربین، میکروفون، مکان یا فایل‌ها را به برنامه می‌دهد.

۳. حملات فیشینگ و لینک‌های آلوده در پیام‌رسان‌ها

- کلیک روی لینک ارسال‌شده در واتساپ، تلگرام یا پیامک که موجب نصب بدافزار یا هدایت به صفحات جعلی می‌شود.

۴. اتصال به وای‌فای و بلوتوث ناامن

- مهاجمان می‌توانند از طریق این کانال‌ها به اطلاعات دستگاه دسترسی پیدا کنند یا بدافزار منتقل کنند.

۵. سوءاستفاده از آسیب‌پذیری‌های سیستم‌عامل

- اگر گوشی به‌روزرسانی‌های امنیتی را دریافت نکند، حفره‌های امنیتی آن باز می‌ماند و امکان نفوذ فراهم می شود.

۶. هک از طریق شارژرهای عمومی (Juice Jacking)

- برخی ایستگاه‌های شارژ عمومی می‌توانند داده‌های شما را هنگام شارژ به سرقت ببرند.

پیامدهای نفوذ

- سرقت اطلاعات شخصی، تصاویر و ویدئوهای خصوصی.
- برداشت غیرمجاز از حساب‌های بانکی.
- جاسوسی از مکالمات و موقعیت مکانی.
- جعل هویت و سوءاستفاده در شبکه‌های اجتماعی.

نشانه‌های آلودگی گوشی

- کاهش شدید سرعت گوشی بدون دلیل مشخص.
- مصرف غیرعادی باتری یا اینترنت.
- نمایش تبلیغات ناخواسته یا پاپ‌آپ‌های مشکوک حتی خارج از مرورگر.
- داغ شدن غیرمعمول دستگاه.
- ارسال پیامک یا تماس به شماره‌های ناشناس بدون اطلاع کاربر.
- تغییرات ناخواسته در تنظیمات گوشی یا نصب اپلیکیشن‌هایی که کاربر آن‌ها را نصب نکرده است.

راهکارهای پیشگیری

۱. نصب اپلیکیشن فقط از منابع معتبر (App Store، Google Play یا بازارهای داخلی معتبر).

۲. بررسی مجوزهای برنامه‌ها پیش از نصب یا هنگام استفاده.

۳. به‌روزرسانی منظم سیستم‌عامل و اپلیکیشن‌ها برای رفع آسیب‌پذیری‌ها.

۴. استفاده از قفل صفحه امن (رمز عبور، اثر انگشت، تشخیص چهره).

۵. خاموش کردن بلوتوث و Wi-Fi در زمان عدم استفاده.

۶. عدم کلیک روی لینک‌های ناشناس در پیام‌ها یا ایمیل‌ها.

۷. پرهیز از استفاده از شارژرهای عمومی یا استفاده از کابل های مخصوص شارژ بدون انتقال داده.

۸. نصب آنتی‌ویروس یا نرم‌افزار امنیتی معتبر موبایل.

اقدامات در صورت مشکوک بودن به نفوذ

- قطع فوری اینترنت گوشی.
- حذف اپلیکیشن‌های ناشناس یا مشکوک.
- اسکن کامل گوشی با اپلیکیشن امنیتی.
- تغییر رمز عبور حساب‌های مهم از دستگاهی امن.
- بازنشانی کارخانه (Factory Reset) در صورت تداوم مشکل.

۲-۶. خانه‌های هوشمند و اینترنت اشیاء (IoT)

خانه هوشمند به مجموعه‌ای از دستگاه‌ها و سامانه‌ها گفته می‌شود که با استفاده از اینترنت، امکان کنترل و مدیریت خودکار بخش‌های مختلف منزل مانند روشنایی، تهویه، امنیت، لوازم خانگی و سرگرمی را فراهم می‌کنند.

اینترنت اشیاء (IoT) مفهومی گسترده‌تر است که شامل اتصال و تبادل داده بین انواع دستگاه‌ها و حسگرها، از خانه‌های هوشمند گرفته تا خودروها، تجهیزات پزشکی و صنعتی، بر بستر اینترنت می‌شود.

تهدیدات رایج

۱. نفوذ به تجهیزات هوشمند
- هکر می‌تواند به دوربین‌های مداربسته، قفل‌های هوشمند یا ترموستات دسترسی پیدا کند و آن‌ها را کنترل یا از داده‌های آن‌ها سوءاستفاده کند.

۲. شنود و جاسوسی
- میکروفون‌های هوشمند، دستیارهای صوتی و حتی تلویزیون‌های هوشمند می‌توانند برای شنود مکالمات یا جمع‌آوری داده‌های شخصی مورد استفاده قرار گیرند.

۳. سرقت داده‌های رفتاری و مکانی
- اطلاعاتی مانند زمان حضور یا عدم حضور شما در منزل، عادات روزانه و مصرف انرژی می‌تواند به مجرمان کمک کند تا حملات فیزیکی یا سایبری برنامه‌ریزی کنند.

۴. حملات به زیرساخت خانه از طریق IoT
- دستگاه‌های آسیب‌پذیر می‌توانند به بخشی از یک بات نت (Botnet) تبدیل شوند و برای حملات گسترده (مانند DDoS) مورد استفاده قرار گیرند.

۵. وابستگی به سرویس‌های ابری
- قطع یا هک شدن سرویس ابری می‌تواند عملکرد کل سیستم خانه هوشمند را مختل کند.

نشانه‌های خطر

- تغییر ناخواسته تنظیمات دستگاه‌های هوشمند.
- روشن یا خاموش شدن خودکار چراغ‌ها، سیستم تهویه یا لوازم خانگی بدون دستور کاربر.
- افزایش غیرمعمول مصرف اینترنت خانگی.
- قطع مکرر ارتباط بین تجهیزات و هاب مرکزی.

راهکارهای پیشگیری

۱. تغییر رمزهای پیش‌فرض دستگاه‌ها
- بسیاری از تجهیزات IoT با رمزهای کارخانه عرضه می شوند که به‌راحتی در اینترنت قابل جستجو هستند.

۲. به‌روزرسانی منظم نرم‌افزار و سیستم‌عامل دستگاه‌ها
- برای رفع آسیب‌پذیری‌های امنیتی شناخته‌شده.

۳. استفاده از شبکه جداگانه برای IoT
- جدا کردن شبکه دستگاه‌های هوشمند از شبکه اصلی اینترنت خانگی.

۴. محدود کردن دسترسی از راه دور
- در صورت عدم نیاز، کنترل از راه دور تجهیزات را غیرفعال کنید.

۵. استفاده از برندها و سرویس‌های معتبر با پشتیبانی امنیتی
- خرید تجهیزات از تولیدکنندگانی که به‌روزرسانی و پشتیبانی امنیتی ارائه می‌دهند.

۶. غیرفعال کردن قابلیت‌های غیرضروری
- مانند دوربین یا میکروفون در دستگاه‌هایی که استفاده نمی‌شوند.

۷. فعال‌سازی رمزگذاری و احراز هویت چندمرحله‌ای
- برای حساب‌های کاربری و اپلیکیشن‌های مرتبط با تجهیزات هوشمند.

اقدامات در صورت بروز مشکل

- قطع فوری اتصال اینترنت تجهیزات مشکوک.
- بررسی تنظیمات و بازگردانی به حالت امن.
- تغییر رمزهای عبور و فعال‌سازی مجدد سرویس‌ها.
- گزارش حادثه به پشتیبانی سازنده یا مراجع ذی‌صلاح.

۲-۷. کلاهبرداری در شبکه‌های اجتماعی

شبکه‌های اجتماعی مانند اینستاگرام، تلگرام، واتساپ، توییتر و لینکدین به بستری گسترده برای ارتباطات شخصی و کاری تبدیل شده‌اند. اما این فضاها علاوه بر مزایا، محل فعالیت گسترده مجرمان سایبری نیز هستند که با استفاده از روش های مهندسی اجتماعی، فیشینگ و تبلیغات فریبنده، اقدام به کلاهبرداری از کاربران می‌کنند.

روش‌های رایج کلاهبرداری در شبکه‌های اجتماعی

۱. پروفایل‌ها و صفحات جعلی

- ایجاد حساب کاربری با نام و تصویر یک فرد یا برند معتبر برای جلب اعتماد دیگران.

نمونه: صفحه‌ای با نام یک فروشگاه معتبر که محصولات تقلبی یا غیرموجود را با قیمت پایین عرضه می‌کند.

۲. قرعه‌کشی‌ها و جوایز جعلی

- وعده برنده شدن در مسابقه یا دریافت هدیه، مشروط به پرداخت هزینه پست یا ثبت اطلاعات بانکی.

۳. فروش کالا یا خدمات غیرواقعی

- آگهی فروش با قیمت پایین برای جلب مشتری، دریافت پول و عدم تحویل کالا.

۴. درخواست کمک مالی یا فوری

- پیام از طرف «دوست» یا «آشنا» که ظاهراً در شرایط اضطراری است و درخواست پول دارد، در حالی که حساب او هک شده است.

۵. لینک‌های آلوده و فیشینگ

- ارسال لینک در پیام خصوصی یا گروه که کاربر را به صفحات جعلی ورود هدایت می‌کند و اطلاعات او را سرقت می‌کند.

۶. سرمایه‌گذاری و ارز دیجیتال جعلی

- وعده سودهای کلان در زمان کوتاه، با استفاده از صفحات تبلیغاتی و چت مستقیم.

نشانه‌های هشداردهنده

- درخواست اطلاعات شخصی یا بانکی در پیام خصوصی.
- پیشنهادهای بیش از حد خوب یا غیرواقعی («کسب درآمد میلیونی در یک هفته»).
- استفاده از دامنه‌ها یا لینک‌های کوتاه‌شده ناشناس.
- تعداد کم پست‌ها یا دنبال‌کننده‌های صفحه نسبت به ادعای بزرگ آن.
- غلط‌های املایی یا نگارشی در پیام‌ها و پست‌ها.

راهکارهای پیشگیری

۱. تأیید هویت صفحات

- دنبال کردن صفحات دارای نشان تأیید (Verified) یا تأیید از طریق وب‌سایت رسمی برند.

۲. عدم ارسال اطلاعات محرمانه در پیام خصوصی

- بانک‌ها، شرکت‌های معتبر و نهادهای رسمی هرگز از طریق پیام خصوصی رمز عبور یا اطلاعات کارت را درخواست نمی‌کنند.

۳. بررسی سابقه فروشنده یا صفحه

- مشاهده نظرات مشتریان، تاریخچه فعالیت و بررسی شماره تماس یا آدرس.

۴. اجتناب از کلیک روی لینک‌های ناشناس

- حتی اگر لینک توسط دوست یا آشنا ارسال شده باشد، ابتدا با او تماس بگیرید و صحت آن را بررسی کنید.

۵. پرداخت امن

- استفاده از درگاه‌های پرداخت معتبر و اجتناب از واریز مستقیم به حساب شخصی ناشناس.

۶. گزارش صفحات مشکوک

- استفاده از گزینه Report در شبکه‌های اجتماعی برای اطلاع‌رسانی به پشتیبانی پلتفرم.

اقدامات در صورت قربانی شدن

- قطع ارتباط فوری با کلاهبردار.
- تغییر رمز عبور حساب‌های کاربری و فعال‌سازی احراز هویت دو مرحله‌ای.
- گزارش موضوع به پلتفرم و مراجع قانونی (مانند پلیس فتا).
- اطلاع‌رسانی به دوستان و دنبال‌کنندگان برای جلوگیری از قربانی شدن سایرین.

۲-۸. تهدیدات ناشی از فناوری‌های نوین

با پیشرفت سریع فناوری، ابزارها و خدمات نوینی وارد زندگی روزمره ما شده‌اند که علاوه بر مزایا، تهدیدات امنیتی و حریم خصوصی جدیدی را نیز ایجاد کرده‌اند.

از جمله این فناوری‌ها می‌توان به هوش مصنوعی (AI)، یادگیری ماشین (ML)، دیپ‌فیک (Deepfake)، بلاک‌چین و ارزهای دیجیتال، رایانش ابری و اینترنت اشیاء (IoT) اشاره کرد. آگاهی از این تهدیدات و روش‌های مقابله با آن‌ها، برای کاربران عادی و سازمان‌ها ضروری است.

مهم‌ترین تهدیدات

۱. دیپ‌فیک (Deepfake)

• استفاده از هوش مصنوعی برای ساخت ویدئو یا صداهای جعلی که به‌طور واقعی به نظر می‌رسند.

کاربردهای مخرب: جعل هویت، تخریب شخصیت، انتشار اخبار جعلی، کلاهبرداری صوتی یا تصویری.

نمونه: تماس تلفنی با صدای تقلیدی مدیرعامل برای انتقال وجه فوری به یک حساب بانکی.

۲. هوش مصنوعی در حملات سایبری

• تولید خودکار ایمیل‌ها یا پیام‌های فیشینگ با کیفیت بالا که شناسایی آن‌ها بسیار دشوار است.

• ساخت بدافزارهایی که رفتار خود را برای دور زدن آنتی ویروس تغییر می‌دهند.

۳. بلاک‌چین و ارزهای دیجیتال

• استفاده از رمزارزها برای تسهیل تراکنش‌های غیرقانونی، پولشویی و دریافت باج در حملات باج‌افزاری.

• کلاهبرداری‌های سرمایه‌گذاری در پروژه‌های ارز دیجیتال بدون پشتوانه (Scam ICOs).

۴. رایانش ابری (Cloud Computing)

• ذخیره داده‌ها در سرورهای خارجی می‌تواند منجر به افشای اطلاعات حساس شود، به‌ویژه در صورت تنظیمات نادرست امنیتی یا هک سرویس‌دهنده.

۵. اینترنت اشیاء (IoT) پیشرفته

• گسترش دستگاه‌های متصل، مانند خودروهای هوشمند یا تجهیزات پزشکی آنلاین، خطر نفوذ و سوءاستفاده را افزایش می‌دهد.

۶. حملات سایبری به زیرساخت‌های حیاتی

• استفاده از فناوری‌های نوین برای نفوذ به سیستم‌های صنعتی، نیروگاه‌ها، شبکه برق و تأسیسات شهری.

نشانه‌های هشداردهنده

• ویدئوها یا صداهایی که رفتار یا گفتار غیرمعمول نسبت به شخصیت اصلی نشان می‌دهند.

• پروژه‌های سرمایه‌گذاری بدون اطلاعات شفاف یا وعده سودهای غیرواقعی.

• ایمیل‌ها یا پیام‌های بسیار حرفه‌ای اما غیرمنتظره.

راهکارهای پیشگیری

۱. آموزش و آگاهی

• آموزش تشخیص محتوای جعلی (Deepfake) و اخبار دروغ.

۲. تأیید چندمرحله‌ای اطلاعات

• پیش از انجام تراکنش‌های مهم یا تصمیمات حساس، هویت درخواست‌کننده را از کانال‌های دیگر تأیید کنید.

۳. استفاده از ابزارهای شناسایی محتوای جعلی

• نرم‌افزارهایی که قادرند تغییرات دیجیتال در ویدئو یا صدا را تشخیص دهند.

۴. مدیریت امن سرویس‌های ابری

• استفاده از رمزگذاری قوی و کنترل دسترسی محدود.

۵. تنوع در روش‌های احراز هویت

• ترکیب رمز عبور، اثر انگشت، کارت هوشمند یا کلید امنیتی.

۶. انتخاب پروژه‌های معتبر در حوزه ارز دیجیتال

• بررسی تیم توسعه، سابقه فعالیت و وجود مجوزهای قانونی.

اقدامات در صورت بروز حادثه

• گزارش فوری به مراجع ذی‌صلاح.

• اطلاع‌رسانی به افراد یا سازمان‌های در معرض خطر.

• بررسی و حذف محتوای جعلی از پلتفرم‌ها در کوتاه‌ترین زمان ممکن.

در این فصل، انواع رایج تهدیدات سایبری که عموم مردم ممکن است با آن‌ها مواجه شوند، معرفی و بررسی شد. از جمله مهم‌ترین آن‌ها می‌توان به فیشینگ و مهندسی اجتماعی اشاره کرد که مهاجمان از طریق جعل هویت یا دستکاری روانی، کاربران را وادار به افشای اطلاعات حساس می‌کنند. باج‌افزار و دیگر بدافزارها نیز تهدیدات جدی هستند که می‌توانند اطلاعات را قفل یا سرقت کنند و خسارات مالی و اعتباری سنگینی به افراد و سازمان‌ها وارد کنند. همچنین، وای‌فای عمومی و حملات شبکه‌ای از جمله مسیرهای نفوذ رایج برای شنود داده‌ها، حملات مرد میانی و ایجاد شبکه‌های جعلی هستند.

تهدیدات دیگری همچون نفوذ به گوشی‌های هوشمند، خانه‌های هوشمند و اینترنت اشیاء (IoT) نیز مورد توجه قرار گرفتند. این دستگاه‌ها که بخشی جدایی‌ناپذیر از زندگی روزمره شده‌اند، در صورت بی‌توجهی به اصول امنیتی می‌توانند منبع جدی افشای داده‌ها، جاسوسی و حتی حملات به زیرساخت‌های حیاتی باشند. کلاهبرداری در شبکه های اجتماعی نیز از دیگر تهدیدات پرشیوع است که با سوءاستفاده از اعتماد کاربران، اقدام به سرقت اطلاعات یا اموال آن‌ها می‌کند.

در پایان، به تهدیدات ناشی از فناوری‌های نوین مانند دیپ‌فیک، حملات مبتنی بر هوش مصنوعی، کلاهبرداری های ارز دیجیتال و سوءاستفاده از رایانش ابری پرداخته شد. این فناوری‌ها با وجود مزایای فراوان، در صورت عدم شناخت و رعایت اقدامات پیشگیرانه می‌توانند به ابزارهای قدرتمند در دست مجرمان سایبری تبدیل شوند. آگاهی عمومی، استفاده از ابزارهای امنیتی مناسب، و پایبندی به شیوه‌های ایمن کاربری، مهم‌ترین راهکارهای مقابله با تمامی این تهدیدات عنوان شد.

فصل سوم

دستورات آمادگی عمومی حین بحران سایبری

بحران سایبری زمانی رخ می‌دهد که یک حمله یا رویداد امنیتی در حال انجام است و به‌طور مستقیم بر داده‌ها، سیستم‌ها یا خدمات حیاتی شما تأثیر می‌گذارد.

دستورات آمادگی عمومی حین بحران سایبری

بحران سایبری زمانی رخ می‌دهد که یک حمله یا رویداد امنیتی در همان لحظه در حال وقوع است و داده‌ها، دستگاه ها یا سرویس‌های حیاتی شما را تحت تأثیر قرار داده است. این بحران می‌تواند از نفوذ به گوشی یا شبکه، قفل شدن فایل ها توسط باج‌افزار، کلاهبرداری آنلاین، یا حتی کنترل غیرمجاز تجهیزات خانه هوشمند شروع شود. در چنین شرایطی، هر ثانیه اهمیت دارد و واکنش درست، می‌تواند مرز میان مهار خسارت و از دست دادن کامل داده‌ها یا سرمایه باشد.

در فصل گذشته، مجموعه‌ای از مهم‌ترین سناریوهای تهدید سایبری که کاربران عادی و سازمان‌ها ممکن است در زندگی روزمره با آن مواجه شوند، به تفصیل بررسی شد. این تهدیدات شامل طیف وسیعی از حملات بودند: فیشینگ و مهندسی اجتماعی که بر فریب روانی کاربر برای افشای اطلاعات حساس تکیه دارند؛ باج‌افزارها و بدافزارها که می‌توانند داده‌ها را قفل کرده یا به سرقت ببرند؛ حملات از طریق شبکه‌های عمومی و وای‌فای که مسیرهای شنود و نفوذ را فراهم می‌کنند؛ نفوذ به گوشی های هوشمند که می‌تواند منجر به کنترل کامل زندگی دیجیتال فرد شود؛ سوءاستفاده از خانه‌های هوشمند و اینترنت اشیاء (IoT) که امنیت فیزیکی و حریم خصوصی را همزمان تهدید می‌کنند؛ کلاهبرداری در شبکه‌های اجتماعی که با جعل هویت یا وعده‌های دروغین به دنبال منافع مالی هستند؛ و در نهایت تهدیدات ناشی از فناوری های نوین مانند دیپ‌فیک، حملات مبتنی بر هوش مصنوعی، کلاهبرداری‌های رمزارزی و سوءاستفاده از رایانش ابری که ابعاد تازه‌ای به جنگ سایبری افزوده‌اند.

با شناخت این تهدیدات، گام بعدی یادگیری این است که در لحظه وقوع یک حادثه سایبری، چه واکنشی باید نشان داد. این فصل دقیقاً بر همین نقطه تمرکز دارد: زمانی که تهدید از مرحله «امکان» گذشته و به «واقعیت» تبدیل شده است. در این لحظات، فرصت تصمیم‌گیری کوتاه است و هر اقدام نادرست می‌تواند به گسترش آلودگی، از بین رفتن دائمی اطلاعات یا حتی سوءاستفاده گسترده‌تر مهاجمان منجر شود.

به همین دلیل، این فصل دستورالعمل‌های عملی و فوری را ارائه می‌کند که بتوانید در زمان مواجهه با هر یک از حملات معرفی‌شده در فصل قبل، به‌سرعت اجرا کنید. این دستورالعمل‌ها شامل اصول واکنش سریع، راهکارهای قطع ارتباط مهاجم، روش‌های ثبت و حفظ شواهد، و اقدامات اختصاصی متناسب با نوع تهدید است. هدف این است که شما بتوانید با کمترین آسیب، بحران را مهار کرده و شرایط را برای بازیابی ایمن سیستم و پیگیری قانونی یا فنی فراهم آورید.

اصول واکنش سریع در زمان بحران سایبری

۱. حفظ آرامش و مدیریت ذهنی
- اولین واکنش طبیعی در بحران، اضطراب و شتاب زدگی است، اما مهاجمان دقیقاً روی همین واکنش حساب می‌کنند.
- چند نفس عمیق بکشید، محیط را ارزیابی کنید و قبل از هر اقدامی، پیامدهای آن را بسنجید.
- هر تصمیم باید بخشی از یک روند منطقی باشد، نه واکنشی احساسی.

۲. ایمن‌سازی فیزیکی و قطع دسترسی مهاجم
- اتصال اینترنت (وای‌فای، داده موبایل، کابل شبکه) را فوراً قطع کنید.
- در حملات مبتنی بر شبکه (مثل مرد میانی یا نفوذ به IoT)، خاموش کردن روتر یا سوئیچ موقتاً ارتباط مهاجم را قطع می‌کند.
- بلوتوث، NFC و هر رابط بی‌سیم دیگر را غیرفعال کنید.

۳. جلوگیری از گسترش آلودگی یا نفوذ
- دستگاه آلوده را به هیچ سیستم، هارد اکسترنال یا فلش دیگری متصل نکنید.
- فایل‌ها یا ایمیل‌های مشکوک را باز نکنید و حتی به عنوان "پیش‌نمایش" مشاهده نکنید.
- در محیط سازمانی، محدوده آلوده را قرنطینه کنید تا شبکه داخلی درگیر نشود.

۴. ثبت، مستندسازی و حفظ شواهد
- هر پیام هشدار، آدرس وب‌سایت، ایمیل مشکوک یا تغییر غیرعادی را ثبت کنید.
- از صفحه‌نمایش، پیام‌ها و تنظیمات تغییر یافته اسکرین‌شات بگیرید.
- یادداشت زمان شروع حادثه و اقدامات انجام شده، بعداً در تحلیل حادثه بسیار ارزشمند است.

۵. اطلاع‌رسانی فوری و هدفمند
- در شرکت‌ها، تیم امنیت، مدیر فناوری یا مدیر ارشد را فوراً در جریان بگذارید.
- در استفاده شخصی، موضوع را به پلیس فتا یا مراکز پاسخگویی حوادث سایبری گزارش دهید.
- اطلاع‌رسانی باید سریع و دقیق باشد تا اقدامات متقابل بدون اتلاف وقت آغاز شود.

۶. اجتناب از تغییر یا حذف داده‌ها بدون مشورت
- حذف فایل‌ها یا ریست کردن دستگاه قبل از تحلیل کارشناسان، می‌تواند شواهد ارزشمند را از بین ببرد.
- در برخی حملات (مثل باج‌افزار)، حذف فایل‌های سیستمی یا تلاش برای بازگردانی دستی می‌تواند داده ها را غیرقابل بازیابی کند.

۷. استفاده از دستگاه یا محیط امن برای ادامه کار
- اگر نیاز به ورود به حساب بانکی یا ایمیل دارید، از دستگاه دیگری که به بحران آلوده نیست استفاده کنید.
- رمزهای عبور مهم را از همان دستگاه امن تغییر دهید.

۸. عدم تعامل با مهاجم
- به پیام‌ها یا درخواست‌های مهاجم پاسخ ندهید، مگر با هماهنگی کارشناس امنیت یا مراجع قانونی.
- حتی پرسیدن سوال یا نشان دادن واکنش می‌تواند به مهاجم اطلاعات بیشتری بدهد.

۹. استفاده از کانال‌های ارتباطی امن
- در زمان بحران، فرض را بر این بگذارید که کانال‌های ارتباطی معمول (ایمیل، پیام‌رسان داخلی یا حتی تماس تلفنی از روی دستگاه آلوده) ممکن است تحت نظارت یا کنترل مهاجم باشد.

اقدامات ویژه برای تهدیدات رایج

فیشینگ (Phishing)

شرح مشکل: فیشینگ روشی است که مهاجم از طریق ایمیل، پیامک، وب‌سایت جعلی یا پیام‌رسان، کاربر را فریب می‌دهد تا اطلاعات حساس خود را وارد کند.

اقدامات در زمان بحران:

- توقف بلافاصله هرگونه تعامل با پیام یا وب‌سایت مشکوک.
- تغییر رمز عبور حساب‌های مرتبط از دستگاه امن.
- بررسی تراکنش‌ها و مسدود کردن کارت بانکی در صورت وارد کردن اطلاعات مالی.
- ذخیره پیام یا لینک جعلی به‌عنوان مدرک.
- گزارش به پلیس فتا یا سامانه‌های گزارش فیشینگ.

مهندسی اجتماعی (Social Engineering)

شرح مشکل: مهندسی اجتماعی شامل فریب یا دستکاری روانی قربانی برای افشای اطلاعات یا انجام عملی خاص است، که می‌تواند از طریق تماس تلفنی، پیام رسان، شبکه اجتماعی یا حتی به‌صورت حضوری انجام شود.

اقدامات در زمان بحران:

- قطع تماس یا مکاتبه با فرد مشکوک.
- تأیید هویت فرد یا سازمان درخواست‌کننده از طریق کانال رسمی مستقل.
- اطلاع‌رسانی به مدیر یا تیم امنیت در صورت وقوع در محیط کاری.
- ثبت جزئیات مکالمه یا پیام‌های دریافتی.
- آموزش و هشدار به اطرافیان برای جلوگیری از حملات مشابه.

باج‌افزار (Ransomware)

شرح مشکل: باج‌افزار نوعی بدافزار است که داده‌های شما را رمزگذاری کرده و برای بازگردانی آن‌ها درخواست باج می‌کند. در بسیاری از موارد، حتی با پرداخت باج نیز تضمینی برای بازیابی داده‌ها وجود ندارد.

اقدامات در زمان بحران:

- قطع فوری ارتباط با اینترنت و شبکه داخلی.
- ذخیره پیام درخواست باج، نمونه فایل‌های رمزگذاری شده و هرگونه مدرک مرتبط.
- مشورت با مراجع فنی یا قانونی قبل از هرگونه پرداخت.
- بازیابی اطلاعات از نسخه پشتیبان سالم.
- اسکن کامل سیستم با ابزارهای امنیتی معتبر پس از حذف تهدید.

نفوذ به گوشی‌های هوشمند

شرح مشکل: مهاجم می‌تواند با نصب بدافزار یا سوءاستفاده از آسیب‌پذیری‌ها، به داده‌ها، دوربین، میکروفون و حتی مکان‌یاب گوشی دسترسی پیدا کند.

اقدامات در زمان بحران:

- فعال‌سازی حالت پرواز (Airplane Mode): این کار بلافاصله ارتباط مهاجم را قطع می‌کند.
- بررسی برنامه‌های نصب‌شده: اپلیکیشن‌های ناشناس یا مشکوک را حذف کنید.
- اسکن امنیتی: از آنتی‌ویروس یا ابزار امنیتی معتبر برای شناسایی و حذف بدافزار استفاده کنید.
- تغییر رمزها از دستگاه دیگر: برای جلوگیری از افشای مجدد، تغییر رمز باید از طریق دستگاهی که آلوده نیست انجام شود.
- بازنشانی کارخانه (Factory Reset): اگر شواهدی از نفوذ عمیق وجود دارد، بازگرداندن گوشی به تنظیمات کارخانه ضروری است.

حمله از طریق وای‌فای عمومی

شرح مشکل: شبکه‌های عمومی می‌توانند ناامن باشند و مهاجمان قادرند داده‌ها را شنود یا نقطه دسترسی جعلی ایجاد کنند.

اقدامات در زمان بحران:

- قطع اتصال فوری.
- غیرفعال کردن اشتراک‌گذاری فایل و سرویس‌های مشابه.
- اسکن سیستم برای یافتن بدافزار.
- تغییر رمز عبور حساب‌های حساس استفاده‌شده در آن شبکه.
- استفاده از VPN معتبر در آینده.

تجهیزات خانه هوشمند و اینترنت اشیاء (IoT)

شرح مشکل: دستگاه‌های هوشمند می‌توانند هدف نفوذ قرار گیرند و کنترل آن‌ها به مهاجم اجازه دهد حتی امنیت فیزیکی را تهدید کند.

اقدامات در زمان بحران:

- قطع اتصال اینترنت یا برق دستگاه.
- بازنشانی به تنظیمات کارخانه.
- تعیین رمز عبور قوی و غیرقابل حدس.
- نصب به‌روزرسانی‌های امنیتی.
- بررسی و حذف دسترسی‌های ناشناس.

اقدامات ویژه‌ای که در این بخش مطرح شد، نه‌تنها برای مهار بحران در لحظه وقوع حادثه کاربرد دارند، بلکه به‌عنوان تجربه ای عملی، آگاهی امنیتی شما را نیز افزایش می‌دهند. هر تهدید سایبری ویژگی‌ها و رفتار خاص خود را دارد، اما وجه مشترک همه آن‌ها این است که در صورت واکنش سریع، دقیق و آگاهانه، می‌توان دامنه خسارت را به حداقل رساند و مسیر بازگشت به شرایط عادی را هموار کرد.

به یاد داشته باشید که مقابله با تهدیدات سایبری، یک رویداد مقطعی نیست؛ بلکه فرایندی مداوم از آمادگی، واکنش و بهبود است. اجرای صحیح این دستورالعمل‌ها، علاوه بر حفظ امنیت داده‌ها و تجهیزات، به شما کمک می‌کند تا در حملات بعدی با اطمینان و توان بیشتری عمل کنید. امنیت سایبری، مسئولیتی مشترک است که از فرد آغاز می‌شود و به کل جامعه گسترش می‌یابد.

نکات کلیدی در حین بحران سایبری

۱. هر اقدام باید هدفمند و حساب‌شده باشد
- در شرایط بحران، تصمیم‌های شتاب‌زده می‌توانند آسیب را بیشتر کنند. قبل از هر اقدامی، چند ثانیه برای ارزیابی وضعیت وقت بگذارید.

۲. همیشه فرض را بر آلودگی بیشتر بگذارید
- حتی اگر تنها یک دستگاه تحت تأثیر قرار گرفته، احتمال گسترش حمله به سایر سیستم‌ها وجود دارد. اقدامات قرنطینه باید سریع و جدی باشد.

۳. از ورود به حساب‌های حساس روی دستگاه مشکوک خودداری کنید
- ورود به ایمیل، شبکه‌های اجتماعی یا حساب بانکی روی سیستمی که احتمال آلودگی دارد، ممکن است رمزها و داده‌های شما را به دست مهاجم برساند.

۴. اطلاعات حساس را فقط از طریق کانال‌های امن منتقل کنید
- اگر لازم است داده یا پیام مهمی ارسال کنید، این کار را از طریق یک دستگاه سالم و با ارتباط رمزگذاری‌شده انجام دهید.

۵. از پاک کردن یا دستکاری شواهد خودداری کنید
- حذف فایل‌ها، ریست کردن دستگاه یا نصب دوباره سیستم‌عامل قبل از تحلیل کارشناسی، می‌تواند روند پیگیری فنی و قانونی را مختل کند.

۶. از حساب‌های پشتیبان و نسخه‌های جایگزین استفاده کنید
- در صورت نیاز به ادامه کار، از یک دستگاه و حساب کاربری جایگزین که از بحران دور نگه داشته شده استفاده کنید.

۷. مهاجم را در جریان اقدامات خود قرار ندهید
- هرگونه پاسخ به پیام مهاجم، حتی به‌صورت کنایه یا تهدید، می‌تواند به او سرنخ بدهد و شرایط را پیچیده‌تر کند.

۸. مستندسازی را در تمام مراحل بحران ادامه دهید
- زمان وقوع رویداد، نوع مشکل، اقدامات انجام‌شده و نتایج هر اقدام را یادداشت کنید تا در آینده بتوانید روند را تحلیل کنید.

۹. همکاری با مراجع قانونی و فنی را جدی بگیرید
- بحران‌های سایبری، به‌ویژه آن‌هایی که منجر به خسارت مالی یا سرقت اطلاعات شده‌اند، باید با همکاری پلیس فتا یا تیم‌های پاسخ‌گویی به حوادث سایبری بررسی شوند.

۱۰. پس از کنترل بحران، درس‌آموخته‌ها را ثبت کنید
- ثبت تجربه‌های عملی و اصلاح سیاست‌های امنیتی، باعث می‌شود در بحران‌های آینده سریع‌تر و دقیق‌تر واکنش نشان دهید.

پدافند سایبری یعنی مجموعه اقدام‌ها برای حفاظت از سرمایه‌های ملی مثل زیرساخت‌های خدمات‌رسان به مردم در برابر تهدیدهای سایبری

فصل چهارم

دستورات آمادگی عمومی پس از بحران سایبری

وقتی یک بحران سایبری کنترل شد یا مهاجم از کار افتاد، ماجرا تمام نشده است. بسیاری از اشتباهات رایج پس از بحران، ناشی از تصور غلط «پایان خطر» است. در واقع، دوره پس از بحران، فرصتی حیاتی برای بازیابی، تحلیل، اصلاح ضعف‌ها و پیشگیری از تکرار حادثه است. در این مرحله، اقدامات شما تعیین می‌کند که آیا بحران یک تجربه آموزنده و تقویت‌کننده خواهد بود یا مقدمه‌ای برای حمله‌ای دوباره.

دستورات آمادگی عمومی پس از بحران سایبری

پایان یک بحران سایبری به معنای پایان تهدید نیست، بلکه آغاز مرحله‌ای حیاتی از بازیابی، تحلیل و پیشگیری است. در فصل‌های پیشین، ابتدا با انواع سناریوهای اصلی تهدیدات سایبری آشنا شدیم و سپس دستورالعمل‌های واکنش فوری در لحظه وقوع بحران را مرور کردیم. اکنون در این فصل، تمرکز ما بر اقداماتی است که پس از کنترل اولیه بحران باید انجام شود؛ اقداماتی که اگر به‌درستی و به‌موقع صورت گیرند، می توانند نه‌تنها اثرات مخرب حمله را کاهش دهند، بلکه احتمال تکرار آن را نیز به حداقل برسانند.

دوره پس از بحران را می‌توان «مرحله ترمیم و مقاوم‌سازی» نامید. در این مرحله، شما فرصت دارید تا داده‌های ازدست‌رفته را بازیابی کنید، آسیب‌پذیری‌های exploited شده را شناسایی و برطرف نمایید، و ساختار امنیتی خود را در برابر تهدیدات آینده تقویت کنید. با این حال، این مرحله نیازمند دقت و نظم بالاست، زیرا اقدامات عجولانه یا ناقص می‌توانند مهاجمان را قادر سازند تا با روش های مشابه یا حتی پیچیده‌تر، حمله‌ای جدید را آغاز کنند.

یکی از بزرگ‌ترین اشتباهات پس از بحران، بی‌توجهی به بررسی علت اصلی حادثه است. بسیاری از سازمان‌ها و حتی کاربران شخصی، پس از بازگشت نسبی سیستم به حالت عادی، به سرعت به روال روزمره بازمی گردند و این امر باعث می‌شود همان خطا یا نقص امنیتی، دوباره تکرار شود. به همین دلیل، این فصل علاوه بر بیان اقدامات فنی مانند اسکن، پاک‌سازی، و تغییر رمزها، بر تحلیل دقیق رویداد، مستندسازی، آموزش و بازنگری سیاست‌های امنیتی نیز تأکید دارد.

در نهایت، باید بدانیم که امنیت سایبری فرآیندی خطی نیست که پس از اجرای چند اقدام به پایان برسد؛ بلکه یک چرخه دائمی از آمادگی، واکنش، بازیابی و بهبود است. این فصل، نقشه راه شما برای عبور هوشمندانه از مرحله «پس از بحران» و تبدیل تجربه تلخ حمله سایبری به فرصتی برای تقویت زیرساخت و افزایش تاب‌آوری خواهد بود.

۱. اطمینان از حذف کامل تهدید

- پس از پایان بحران، اولین گام این است که مطمئن شوید عامل تهدید به‌طور کامل حذف شده است. این کار باید با اسکن جامع سیستم‌ها و شبکه، استفاده از ابزارهای امنیتی به‌روز و بررسی دستی پوشه‌ها و فرآیندهای مشکوک انجام شود.
- هرگونه بدافزار، کد مخرب یا تغییرات غیرمجاز در تنظیمات سیستم باید شناسایی و حذف شود.
- اگر کوچک‌ترین تردیدی در پاک‌سازی کامل وجود دارد، نصب مجدد سیستم‌عامل توصیه می‌شود.

۲. بازیابی امن داده‌ها و سرویس‌ها

- برای بازگرداندن اطلاعات، تنها از نسخه‌های پشتیبان سالم که قبل از وقوع حادثه تهیه شده‌اند استفاده کنید.
- قبل از بازیابی، فایل‌های پشتیبان را نیز اسکن کنید تا مطمئن شوید آلودگی به آن‌ها منتقل نشده است.
- بازیابی باید به‌صورت مرحله‌ای انجام شود تا در صورت بروز مشکل، بتوان منبع آلودگی را سریعاً شناسایی کرد.

۳. تغییر کامل رمزها و فعال‌سازی احراز هویت چندمرحله‌ای

- همه رمزهای عبور، حتی آن‌هایی که تصور می‌کنید افشا نشده‌اند، باید تغییر کنند.
- از رمزهای طولانی، ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها استفاده کنید.
- در تمام سرویس‌های حساس، احراز هویت چندمرحله ای (MFA) فعال شود تا در صورت سرقت رمز، ورود غیرمجاز امکان‌پذیر نباشد.

۴. تحلیل ریشه‌ای حادثه (Root Cause Analysis)

- بررسی کنید که مهاجم از چه روشی وارد شده است (ایمیل فیشینگ، آسیب‌پذیری نرم‌افزار، ضعف پیکربندی و غیره).
- شناسایی دقیق نقطه ضعف به شما کمک می‌کند که در آینده آن را برطرف کرده و مانع حملات مشابه شوید.
- اگر امکان دارد، از گزارش‌های فنی تیم امنیت یا شرکت های متخصص استفاده کنید.

۵. اطلاع‌رسانی به ذی‌نفعان و مراجع قانونی
- اگر اطلاعات حساس مشتریان یا کارکنان افشا شده است، باید آن‌ها را مطلع کنید تا اقدامات محافظتی لازم را انجام دهند.
- در حملات جدی، گزارش‌دهی به پلیس فتا و سایر مراجع قانونی الزامی است.
- شفافیت در اطلاع‌رسانی باعث جلب اعتماد و جلوگیری از انتشار شایعات می‌شود.

۶. مستندسازی و ثبت درس‌آموخته‌ها
- تمام جزئیات بحران، از اولین نشانه‌ها تا اقدامات پایانی، باید مکتوب و بایگانی شود.
- این مستندات می‌توانند در آموزش کارکنان، بازبینی سیاست‌ها و بهبود واکنش‌های آینده استفاده شوند.
- درس‌آموخته‌ها باید در قالب دستورالعمل یا چک‌لیست به تیم‌ها ابلاغ شوند.

۷. به‌روزرسانی سیاست‌های امنیتی و سخت‌افزاری
- قوانین دسترسی کاربران، استفاده از تجهیزات جانبی، و خط‌مشی‌های ارتباطات اینترنتی را بازبینی و اصلاح کنید.
- نرم‌افزارها و سیستم‌ها باید به آخرین نسخه ارتقاء یابند تا حفره‌های امنیتی شناخته‌شده بسته شوند.
- در صورت نیاز، ابزارها و تجهیزات امنیتی جدید خریداری یا ارتقاء داده شوند.

۸. آموزش و فرهنگ‌سازی امنیتی
- برگزاری دوره‌های آموزشی برای کارکنان یا اعضای خانواده درباره تهدیدات مشابه و راه‌های پیشگیری.
- استفاده از مثال واقعی حادثه اخیر برای افزایش حساسیت و آمادگی ذهنی.
- آموزش باید مستمر و به‌روز باشد، نه صرفاً یک‌بار پس از بحران.

۹. نظارت فعال و آماده‌باش مداوم
- فعال‌سازی سیستم‌های نظارتی و هشداردهی برای شناسایی سریع فعالیت‌های مشکوک.
- بررسی منظم گزارش‌های امنیتی، لاگ‌ها و وضعیت سلامت سیستم‌ها.
- انجام تست نفوذ دوره‌ای برای ارزیابی آمادگی در برابر حملات آینده.

دوره پس از بحران سایبری، یک فرصت طلایی برای افزایش مقاومت و تاب‌آوری در برابر تهدیدات آینده است. برخورد فعال، ثبت تجربیات و اصلاح ضعف ها باعث می‌شود که هر حمله، به جای یک شکست، به سکوی پیشرفت امنیتی تبدیل شود. به یاد داشته باشید که امنیت یک نقطه پایان ندارد؛ بلکه فرایندی دائمی از پیشگیری، پاسخ و بهبود است.

فصل پنجم

رایج ترین اشتباهات کاربران در حوزه پدافند سایبری

بخش بزرگی از موفقیت حملات سایبری نه به دلیل پیچیدگی فنی مهاجمان، بلکه به دلیل اشتباهات ساده و قابل پیشگیری کاربران است. در این فصل، به مهم‌ترین خطاهایی می‌پردازیم که در حوزه امنیت اطلاعات و پدافند سایبری رایج‌اند و راهکارهایی برای پرهیز از آن‌ها ارائه می‌کنیم. هدف این است که با شناخت این دام‌ها، از افتادن در آن‌ها جلوگیری کنیم.

رایج‌ترین اشتباهات کاربران

در حوزه پدافند سایبری

یکی از اصلی‌ترین دلایل موفقیت حملات سایبری، پیچیدگی فنی یا قدرت بالای مهاجمان نیست، بلکه اشتباهات ساده، تکراری و قابل پیشگیری کاربران است. این واقعیت در بررسی‌های بسیاری از حوادث امنیتی به اثبات رسیده است؛ جایی که عامل نفوذ نه یک نقص نرم‌افزاری پیچیده، بلکه یک کلیک بی‌جا روی یک لینک مشکوک، انتخاب یک رمز عبور ضعیف، یا نادیده گرفتن یک هشدار امنیتی بوده است.

در فصل‌های پیشین این کتابچه، با سناریوهای اصلی تهدیدات سایبری و شیوه‌های واکنش پیش و حین بحران آشنا شدیم. اکنون زمان آن رسیده که به وجه انسانی امنیت سایبری بپردازیم؛ همان نقطه‌ای که مهاجمان بارها و بارها از آن سوءاستفاده کرده‌اند. تجربه نشان داده که حتی سازمان هایی که از پیشرفته‌ترین تجهیزات امنیتی و زیرساخت‌های فنی استفاده می‌کنند، در برابر یک اشتباه انسانی کوچک می‌توانند دچار خسارات سنگین شوند.

اشتباهات امنیتی نه‌تنها در بین کاربران عادی، بلکه در میان مدیران، کارشناسان و حتی متخصصان حوزه فناوری اطلاعات نیز دیده می‌شود. دلیل این امر ساده است: انسان ها ذاتاً تمایل دارند راحتی و سرعت را بر دقت و امنیت ترجیح دهند. برای مثال، استفاده از یک رمز عبور ساده و تکراری ممکن است چند ثانیه در زمان ورود صرفه‌جویی کند، اما می تواند در آینده منجر به افشای گسترده اطلاعات و حتی از دست رفتن سرمایه‌های مالی شود.

هدف این فصل، ارائه فهرستی از رایج‌ترین اشتباهات در حوزه پدافند سایبری و توضیح دقیق پیامدهای هرکدام است تا خواننده بتواند آن‌ها را شناسایی کرده و از تکرارشان جلوگیری کند. با شناخت این خطاها و به‌کارگیری راهکارهای عملی، می‌توان سطح ایمنی فردی و سازمانی را به‌طور قابل توجهی افزایش داد. در حقیقت، پرهیز از اشتباهات رایج، همان‌قدر اهمیت دارد که اجرای اقدامات پیشگیرانه و واکنش سریع در زمان بحران.

۱. استفاده از رمزهای عبور ضعیف و تکراری

- انتخاب رمزهای ساده مثل «۱۲۳۴۵۶» یا «Aa۱۱۱۱۱» یکی از رایج‌ترین خطاهاست.
- استفاده از یک رمز برای چندین حساب کاربری، باعث می‌شود با لو رفتن یک رمز، مهاجم به بقیه حساب‌ها هم دسترسی پیدا کند.

راهکار: استفاده از رمزهای قوی، منحصربه‌فرد و مدیریت شده توسط نرم‌افزارهای معتبر مدیریت رمز عبور.

۲. بی‌توجهی به به‌روزرسانی نرم‌افزار و سیستم‌ها

- بسیاری از حملات سایبری از طریق آسیب‌پذیری‌های شناخته‌شده در نسخه‌های قدیمی نرم‌افزار انجام می شود.

راهکار: فعال‌سازی به‌روزرسانی خودکار یا بررسی منظم نسخه‌های جدید نرم‌افزارها و نصب به‌روزرسانی‌های امنیتی.

۳. کلیک روی لینک‌ها و فایل‌های ناشناس

- باز کردن ایمیل‌ها یا پیام‌های مشکوک و دانلود فایل‌های ناشناس، یکی از اصلی‌ترین روش‌های ورود بدافزار به سیستم است.

راهکار: بررسی فرستنده، استفاده از ابزارهای اسکن لینک، و باز نکردن فایل‌هایی که منبع آن‌ها مشخص نیست.

۴. استفاده از وای‌فای عمومی بدون محافظت

- اتصال به شبکه‌های باز در کافی‌شاپ، فرودگاه یا مکان های عمومی بدون VPN، می‌تواند اطلاعات شما را در معرض شنود قرار دهد.

راهکار: استفاده از VPN معتبر و اجتناب از ورود به حساب های حساس روی شبکه‌های عمومی.

۵. نادیده گرفتن هشدارهای امنیتی مرورگر یا آنتی ویروس

- بسیاری از کاربران هشدارهای «سایت ناامن» یا «فایل مشکوک» را نادیده گرفته و ادامه می‌دهند.

راهکار: جدی گرفتن هشدارها و قطع تعامل با منبع مشکوک تا بررسی کامل انجام شود.

۶. اشتراک‌گذاری بیش‌ازحد اطلاعات شخصی در شبکه‌های اجتماعی

- انتشار تاریخ تولد، آدرس، محل کار و سایر اطلاعات شخصی می‌تواند توسط مهاجمان برای حملات مهندسی اجتماعی استفاده شود.

راهکار: محدود کردن میزان اطلاعات قابل مشاهده برای عموم و استفاده از تنظیمات حریم خصوصی.

۷. عدم پشتیبان‌گیری منظم از داده‌ها

- نبود نسخه پشتیبان، در صورت حمله باج‌افزاری یا خرابی سیستم، باعث از دست رفتن کامل اطلاعات می شود.

راهکار: پشتیبان‌گیری منظم روی حافظه خارجی یا فضای ابری امن و جدا از شبکه اصلی.

۸. اعتماد بی‌جا به تماس‌ها یا پیام‌های فوری

- مهاجمان با ایجاد حس فوریت («حساب شما مسدود می شود» یا «بلافاصله رمز را بدهید») قربانی را وادار به اقدام سریع و بدون فکر می‌کنند.

راهکار: توقف، بررسی و تأیید هویت درخواست‌کننده قبل از هر اقدام.

۹. غیرفعال کردن یا حذف نرم‌افزارهای امنیتی

- برخی کاربران برای افزایش سرعت سیستم، آنتی‌ویروس یا فایروال را غیرفعال می‌کنند که این کار یک اشتباه جدی است.

راهکار: استفاده از نرم‌افزارهای امنیتی معتبر و فعال نگه داشتن آن‌ها در همه حال.

اشتباهات امنیتی کوچک می‌توانند پیامدهای بزرگی داشته باشند. آگاهی، دقت و رعایت اصول ساده امنیتی می‌تواند از وقوع بسیاری از تهدیدات سایبری جلوگیری کند. پدافند سایبری یک مسئولیت فردی و جمعی است که با پرهیز از این اشتباهات، قدم مهمی در حفظ امنیت دیجیتال خود و دیگران برمی‌داریم.