به نام خدا

چک‌لیست اقدامات حقوقی پس از حمله سایبری به کسب‌وکار

تهیه و تنظیم:مینا خالقی

این چک‌لیست برای استفاده فوری پس از وقوع یا کشف حمله سایبری طراحی شده است.

گام‌ها به ترتیب اولویت مرتب شده‌اند.

🔴**فوری — بحرانی:** باید ظرف ۱ تا ۴ ساعت انجام شود

☐**چک‌باکس:** پس از انجام تیک بزنید

فاز ۱ ساعت اول: مهار و ایمن‌سازی فوری

اقدامات بحرانی که نباید تأخیر داشته باشند

☐	**ایزوله کردن سیستم‌های آلوده از شبکه** کابل شبکه را جدا کنید / Wi-Fi را غیرفعال کنید — سیستم را خاموش نکنید
☐	**تغییر فوری رمزهای عبور مدیریتی** حساب‌های Admin، ایمیل سازمانی، پنل بانکی، و VPN را ریست کنید
☐	**مسدود کردن حساب‌های بانکی در معرض خطر** با بانک تماس بگیرید و درخواست انجماد تراکنش‌های مشکوک دهید
☐	**اطلاع به تیم امنیت IT یا ارائه‌دهنده خدمات امنیتی** اگر تیم داخلی ندارید، با یک شرکت امنیت سایبری تماس بگیرید
☐	**شروع ثبت گزارش زمانی (Incident Log)** تاریخ، ساعت، توصیف رویداد و نام شخص اقدام‌کننده را یادداشت کنید
☐	**تهیه اسکرین‌شات از پیام‌های مهاجم یا باج‌افزار** قبل از هر اقدام دیگری، صفحه را عکس بگیرید — متن پیام را تایپ کنید

⚠️ ⚠️ **هرگز سیستم آلوده را قبل از تهیه لاگ و گزارش فنی**

خاموش یا ری‌استارت نکنید.

خاموش کردن می‌تواند شواهد دیجیتال حیاتی را

از بین ببرد. ⚠️ ⚠️

فاز ۲ ۴ تا ۲۴ ساعت: مستندسازی دیجیتال

جمع‌آوری و حفاظت از مدارک فنی

☐	**استخراج و ذخیره لاگ‌های سرور** لاگ‌های سیستم‌عامل، وب‌سرور، فایروال و IPS/IDS را در رسانه جداگانه ذخیره کنید
☐	**استخراج هدرهای کامل ایمیل‌های مشکوک** در پرونده‌های فیشینگ: Full Headers را ذخیره کنید (نه فقط To/From)
☐	**ثبت آدرس‌های IP مشکوک** تمام IP ارتباطی با مهاجم را یادداشت کنید — از ابزار whois استفاده نمایید
☐	**قرنطینه نمونه بدافزار یا فایل آلوده** فایل مشکوک را در پوشه رمزدار فشرده کنید — به هیچ سیستمی کپی نشود
☐	**تهیه هش رمزنگاری از مدارک (SHA-۲۵۶)** از ابزار CertUtil یا sha۲۵۶sum برای ثبت یکپارچگی مدارک استفاده کنید
☐	**ذخیره آدرس کیف‌پول رمزارز مهاجم** در پرونده باج‌افزاری: آدرس کامل wallet را ثبت کنید — برای پیگیری بعدی ضروری است
☐	**تهیه گزارش فنی اولیه از کارشناس IT** گزارش مکتوب با توصیف فنی رویداد، نقاط ورود احتمالی، و سیستم‌های آسیب‌دیده

نکته حقوقی:

زنجیره حفاظت از مدارک (Chain of Custody) در دادگاه‌های ایران اهمیت فزاینده‌ای دارد.

تمام مدارک دیجیتال باید با ثبت زمان، نام جمع‌کننده، و هش رمزنگاری مستند شوند.

فاز ۳ ۲۴ تا ۷۲ ساعت: اقدامات حقوقی رسمی

آغاز فرایند قضایی و اطلاع‌رسانی قانونی

☐	**ثبت شکایت در پلیس فتا** مراجعه به Cyberpolice.ir یا دفتر پلیس فتا — دریافت شماره پیگیری الزامی است
☐	**تنظیم شکوائیه رسمی با کمک وکیل متخصص** شکوائیه باید شامل توصیف دقیق جرم، مواد قانونی مستدل، و فهرست مدارک باشد
☐	**درخواست دستور موقت قضایی (در صورت لزوم)** برای توقف انتشار اطلاعات افشاشده یا مسدود کردن دسترسی — از طریق دادسرا
☐	**اطلاع به ارائه‌دهنده خدمات اینترنت (ISP)** برای مسدود کردن IP مهاجم یا IP مخرب — می‌تواند مکمل اقدام قضایی باشد
☐	**ارجاع پرونده به کارشناس رسمی دادگستری رشته انفورماتیک** اخذ نظریه کارشناسی برای اثبات خسارت و احراز ارکان جرم در مرحله دادرسی
☐	**تنظیم صورتجلسه داخلی مدیریت** مستندسازی رسمی رویداد در سوابق شرکت — برای موارد مسئولیت آتی ضروری است

فاز ۴ اطلاع‌رسانی به ذی‌نفعان

تعهدات قانونی اطلاع‌رسانی — طبق قانون تجارت الکترونیک

☐	**اطلاع به مشتریانی که داده‌هایشان افشا شده** ماده ۵۸ قانون تجارت الکترونیک — در اسرع وقت ممکن؛ تأخیر می‌تواند موجب مسئولیت مضاعف شود
☐	**اطلاع به شرکای تجاری در معرض خطر** شرکای B۲B که اطلاعاتشان ممکن است در سیستم شما بوده، باید مطلع شوند
☐	**اطلاع به بانک و مؤسسات مالی ذی‌ربط** ارائه گزارش حمله به بانک — ضروری برای پیگیری تراکنش‌های مشکوک
☐	**ارائه گزارش به هیئت مدیره و سهامداران** در شرکت‌های سهامی: افشاء رویداد مهم امنیتی می‌تواند تکلیف قانونی باشد
☐	**اطلاع به بیمه‌گر (در صورت داشتن بیمه سایبری)** تأخیر در اطلاع‌رسانی به بیمه‌گر می‌تواند حق مطالبه خسارت را ساقط کند
☐	**آماده‌سازی بیانیه عمومی (در صورت نیاز به افشاء رسانه‌ای)** مشورت با وکیل قبل از هر اظهار عمومی — از اعترافاتی که بار اثبات را تغییر دهند پرهیز کنید

هشدار:

هرگز بدون مشورت وکیل متخصص بیانیه عمومی یا مصاحبه رسانه‌ای درباره حمله سایبری نداشته باشید.

اظهارات غیرمحتاطانه می‌توانند در دادرسی علیه شما استفاده شوند.

فاز ۵ بازیابی و پیشگیری

استحکام‌بخشی حقوقی و فنی برای جلوگیری از تکرار

☐	**بازیابی سیستم‌ها از نسخه پشتیبان سالم** قبل از اتصال مجدد به شبکه، سیستم باید کاملاً پاک‌سازی و بررسی شده باشد
☐	**ممیزی امنیتی کامل (Security Audit)** ارزیابی کلیه آسیب‌پذیری‌ها توسط متخصص مستقل — مستندسازی نتایج الزامی است
☐	**بازنگری و به‌روزرسانی سیاست‌های امنیتی** دستورالعمل‌های داخلی، رمزهای عبور، دسترسی‌ها و پروتکل‌های امنیتی را مرور کنید
☐	**آموزش مجدد کارکنان درباره امنیت سایبری** تأکید ویژه بر شناسایی فیشینگ و مهندسی اجتماعی
☐	**بازنگری قراردادهای IT و ارائه‌دهندگان خدمات** بررسی SLA ها و تعهدات امنیتی — اضافه کردن بندهای مسئولیت سایبری
☐	**ارزیابی امکان مطالبه خسارت از اشخاص ثالث** در صورتی که ضعف امنیتی مربوط به نرم‌افزار یا سرویس شخص ثالث باشد
☐	**تدوین یا به‌روزرسانی برنامه واکنش به حوادث (IRP)** برنامه مکتوب که نقش‌ها، مسئولیت‌ها و مراحل اقدام را مشخص کند

فهرست مدارک ضروری برای شکایت

نوع مدرک	توضیح / نکات مهم
لاگ‌های سرور	با تاریخ و آدرس IP — باید هش‌گذاری شوند
هدرهای کامل ایمیل	ویژه پرونده‌های فیشینگ — نه فقط متن
گزارش فنی کارشناس IT	مکتوب، امضاشده، با ذکر تخصص کارشناس
نمونه بدافزار قرنطینه‌شده	در فایل فشرده رمزدار — تحویل به پلیس فتا
مدارک خسارت مالی	فاکتور، برگه بانکی، گزارش حسابداری
مدارک شرکت (روزنامه رسمی)	اثبات شخصیت حقوقی شاکی
آدرس کیف‌پول رمزارز	ویژه پرونده‌های باج‌افزار — برای ردیابی
اسکرین‌شات‌های مستند	با ثبت تاریخ و ساعت دقیق
ارتباطات با مهاجم	ایمیل، پیامک، کانال‌های Telegram یا Dark Web

مواد قانونی کلیدی برای استناد

- ماده ۱ ق.ج.ر ۱۳۸۸ — دسترسی غیرمجاز
- ماده ۸ و ۹ — اختلال در سیستم‌ها
- ماده ۱۰ — تخریب داده‌ها
- ماده ۱۳ — کلاهبرداری رایانه‌ای
- ماده ۵۸ ق.ت.ا — حفاظت از داده شخصی
- ماده ۶۶۹ ق.م.ا — تهدید و اخاذی
- مواد ۲۲۱ و ۳۳۵ ق.م. — مسئولیت مدنی

از حسن توجه شما عزیزان متشکریم

تهیه و تنظیم:مینا خالقی