دادبان

راهنمای
امنیت دیجیتال
ویژه وکلا و حقوق‌دانان

دادبان

راهنمای
امنیت دیجیتال

ویژه وکلا و حقوق‌دانان

راهنمای امنیت دیجیتال
ویژه وکلا و حقوق‌دانان

دادبان؛ مرکز مشاوره و آموزش حقوقی ویژه کنش‌گران

درآمد

هدف این راهنما چیست؟

هدف این راهنما ارائه توصیه‌های اساسی در زمینه امنیت دیجیتال به وکلا است تا اطلاعات حساس و حریم شخصی مراجعه‌کنندگان را حفظ کرده و از نفوذ داده‌ها، حملات سایبری و دسترسی غیرمجاز جلوگیری نمایند.

اهمیت امنیت دیجیتال برای وکلا

به عنوان وکیل و حقوق‌دان، شما به صورت مداوم با اطلاعات حساس و محرمانه مراجعه‌کنندگان سروکار دارید. تضمین امنیت این اطلاعات امری بسیار حیاتی است. امنیت دیجیتال برای مقابله با نفوذ داده، حملات سایبری و دسترسی غیرمجاز به این دست اطلاعات بسیار مهم است.

مدیریت رمز عبور

رمز عبور قدرتمند

- از رمزهای عبور پیچیده با ترکیبی از حروف بزرگ و کوچک، اعداد و نمادهای خاص استفاده کنید.
- از استفاده از رمز عبورهایی که یا حاوی اطلاعات شخصی شماست - همچون تاریخ تولد - یا جزء کلمات رایج است، خودداری کنید.
- رمزهای عبور خود را به صورت دوره‌ای تغییر دهید.

تایید هویت دومرحله‌ای (2FA)

- در هر سرویسی که امکان دارد، تایید هویت دومرحله‌ای(2FA) را فعال کنید تا یک لایه امنیتی بیش‌تر ایجاد کنید.
- از برنامه‌های تایید هویت دو مرحله‌ای برای دریافت کد یکبار مصرف یا کلیدهای سخت‌افزاری برای ۲FA استفاده کنید.
- اگر در ایران هستید از اپلیکیشن Authenticator برای دریافت کد استفاده کنید.

اپلیکیشن‌های مدیریت رمز عبور

- از یک برنامه مدیریت رمز عبور قابل اعتماد برای ذخیره و تولید رمزهای عبور پیچیده استفاده کنید.
- اطمینان حاصل کنید که خود برنامه مدیریت رمز عبور نیز به واسطه یک رمز عبور قدرتمند محافظت شده باشد. رمز عبور این برنامه را به هیچ عنوان فراموش نکنید.

ارتباط امن

رمزگذاری

- برای همه ارتباطات و برای امنیت به‌اشتراک‌گذاری داده‌ها از رمزگذاری end-to-end استفاده کنید.
- اطمینان حاصل کنید که ابزارهای ارتباطی و نرم‌افزارهای ایمیل شما از سیستم رمزگذاری استفاده می‌کنند.

ایمیل امن

- از خدمات ایمیل‌های رمزگذاری شده مانند پروتون ایمیل (proton mail) استفاده کنید.
- مراقب پیوست‌ها و لینک‌های ایمیل‌ها باشید، چرا که ممکن است حاوی نرم‌افزارهای مخرب باشند.
- ایمیل‌ها را به صورت منظم و دوره‌ای پاک کنید. ایمیلی که حاوی اطلاعات مهم است را اصلا نگهداری نکنید و حتما پس از استفاده پاک کنید.

پیام‌رسان‌های رمزگذاری‌شده

- در نظر بگیرید از پیام‌رسان‌های رمزگذاری‌شده برای مکالمات حساس استفاده کنید.
- قبل از اشتراک گذاری مطالب مطمئن شوید ادرس ایمیل کاربر و اطلاعات کاربر درست است و به اشتباه اطلاعات حساس را برای کاربران دیگر به اشتراک نگذارید.
- تاریخچه گفتگوها در پیام‌رسان‌ها را به صورت منظم و دوره‌ای پاک کنید.

دستگاه‌ها و شبکه‌های امن

امنیت دستگاه‌ها

- سیستم‌عامل دستگاه‌ها (کامپیوترها، تلفن‌های هوشمند، تبلت‌ها) را به‌روز کنید.
- نرم‌افزارهای معتبر ضد ویروس و ضد بدافزار نصب کنید.
- رمزگذاری دیسک (فضای ذخیره‌سازی دستگاه) کامل را فعال کنید.

شبکه‌های امن وای‌فای

- برای شبکه‌های وای‌فای از رمزهای عبور قوی و منحصر بفرد استفاده کنید.
- سرویس‌های شبکه وای‌فای غیرضروری را غیرفعال کنید.
- بهتر است به شبکه‌های وای‌فای عمومی متصل نشوید.
- برای امنیت بیش‌تر حتما از یک وی‌پی‌ان امن استفاده کنید.

پشتیبانی و بازیابی اطلاعات

پشتیبانی منظم

- به طور منظم از اطلاعات مهم‌تان نسخه پشتیبان تهیه کنید.
- برای اطمینان از کارایی لازم، روند بازیابی اطلاعات را تست کنید.

بازیابی اطلاعات

- یک برنامه بازیابی اطلاعات تهیه کنید که در صورت ازدست‌دادن اطلاعات بتوانید آن‌ها را آسان بازیابی کنید.

حفاظت از اطلاعات مراجعه‌کنندگان

رعایت حریم خصوصی مراجعه‌کنندگان

- از حریم خصوصی مراجعه‌کنندگان به‌شدت مراقبت کنید و از به‌اشتراک‌گذاری نمونه‌ها و پرونده‌ها در فضای مجازی - حتی بدون ذکر مشخصات فردی - خودداری کنید.
- دسترسی به اطلاعات مهم مراجعه‌کنندگان - که در فایل‌ها یا فولدرها قرار دارند - را محدود کنید.

ذخیره‌سازی امن اسناد

- از فضاهای ابری امن برای ذخیره‌سازی اسناد و فایل‌های مهم مراجعه‌کنندگان استفاده کنید و حتما به صورت رمزگذاری شده ذخیره کنید.
- اگر از حافظه دستگاه و یا هارد استفاده می‌کنید ابتدا فایل‌ها را رمزگذاری کنید، سپس ذخیره و بایگانی کنید.

به‌اشتراک‌گذاری و همکاری

- برای به‌اشتراک‌گذاری، از برنامه‌های امن استفاده کنید؛ مانند گوگل درایو - وان‌درایو و دراپ‌باکس.

آگاهی از مهندسی اجتماعی (امنیت)

حملات فیشینگ

- مراقب ایمیل‌های فیشینگ باشید و از هویت فرستنده‌ها اطمینان حاصل کنید.
- به هیچ عنوان فایل‌ها و لینک‌های ایمیل‌های مشکوک به فیشینگ را کلیک و دانلود نکنید.
- به محتوای ایمیل‌های مشکوک به فیشینگ دقت کنید؛ معمولا حاوی اطلاعات اشتباه و غلط‌های املایی هستند.

حملات فیشینگ و تقلب در هویت

- در مورد تماس‌ها یا پیام‌های تلفنی ناخواسته که اطلاعات حساس را درخواست می‌کنند، مراقب باشید.
- پیش از به‌اشتراک‌گذاری اطلاعات، از هویت تماس‌گیرندگان، اطمینان حاصل کنید.

نکته واپسین

با به‌کارگیری توصیه‌های این راهنما، وکلا می‌توانند ریسک‌های مرتبط با تهدیدات دیجیتال را به حداقل برسانند، از اطلاعات حساس مراجعه‌کنندگان محافظت کنند و استانداردهای بالاتری از اخلاق حرفه‌ای را در عمل پیاده کنند.