امنیت اطلاعات

کارمندان حلقه اصلی امنیت در سازمان ها

علی محمد رجبی

دی ماه ۱۴۰۰

علی محمد رجبی

پژوهشگر در حوزه فضای مجازی

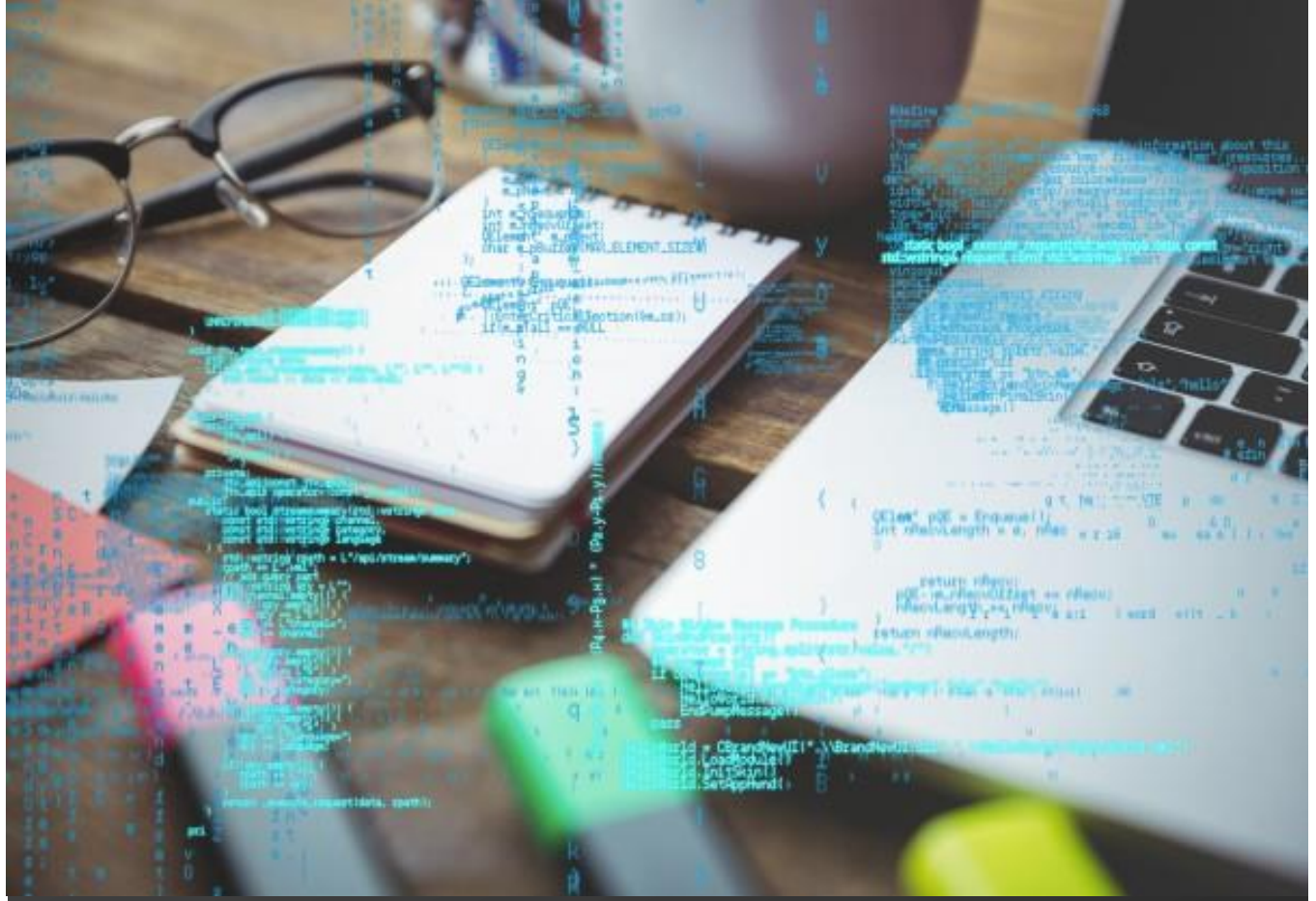
info@familyweb.ir

familyweb.ir

نقش کارکنان در حفظ امنیت اطلاعات

در هزاره سوم، اطلاعات مهمترین مزیت رقابتی هر سازمان است.

این داده ها و اطلاعات هستند که می توانند برای هر مجموعه ای قدرت تصمیم گیری، مدیریت، اجرای ماموریت و تداوم فعالیت را فراهم کنند.



اهمیت اطلاعات در دسترس ما

هر کارمند، مسئول یا مدیر با توجه به جایگاه خود دسترسی به اطلاعاتی دارد. **اطلاعات** در دسترس ما **دارایی های حیاتی سازمان** است و از دست دادن آنها و یا دسترسی افراد سودجو به آنها ممکن است جبران ناپذیر باشد.

امنیت اطلاعات چیست

امنیت اطلاعات فرآیند محافظت از داده های الکترونیکی و چاپی، تجهیزات الکترونیکی و شبکه یا هر نوع محرمانه دیگری از داده ها در برابر حملات و دسترسی های غیر مجاز است.

82 درصد از کارفرمایان از کمبود مهارت های حرفه ای لازم برای محافظت از تهدیدات امنیت اطلاعات در بین کارکنانشان خبر می دهند.

امنیت اطلاعات به زبان ساده

ضرورت کسب مهارت امنیتی در کارکنان

۱ – برای یک مهاجم آسانتر است که کارمندی را وادار به کلیک بر روی یک پیوند آلوده و یا نصب بدافزار کند تا بخواهد از لایه های امنیتی شرکت عبور کند.

۲ – هیچ برنامه امنیتی بدون مشارکت کارمندان موفق نخواهد بود.

۳– کارکنان سازمان در هر سطحی از مدیران ارشد تا کارمندان ساده متناسب با سطح دسترسی شان به اطلاعات و تجهیزات، با تهدیدات متفاوتی مواجه هستند.

رایج ترین تهدیدات سایبری به ترتیب اولویت

۱. حملات بدافزاری
۲. حملات تحت وب
۳. فیشینگ
۴. حملات نرم افزارهای تحت وب
۵. هرزنامه
۶. حملات منع سرویس توزیع شده
۷. سرقت هویت
۸. نقض داده ها
۹. تهدید از داخل سازمان
۱۰. بات نت
۱۱. آسیب دیدن و یا سرقت تجهیزات
۱۲. نشت اطلاعات
۱۳. باج افزار
۱۴. جاسوسی سایبری
۱۵. استخراج غیر مجاز رمزارز

حوزه های تاثیرگذاری کارمندان بر امنیت اطلاعات سازمانی

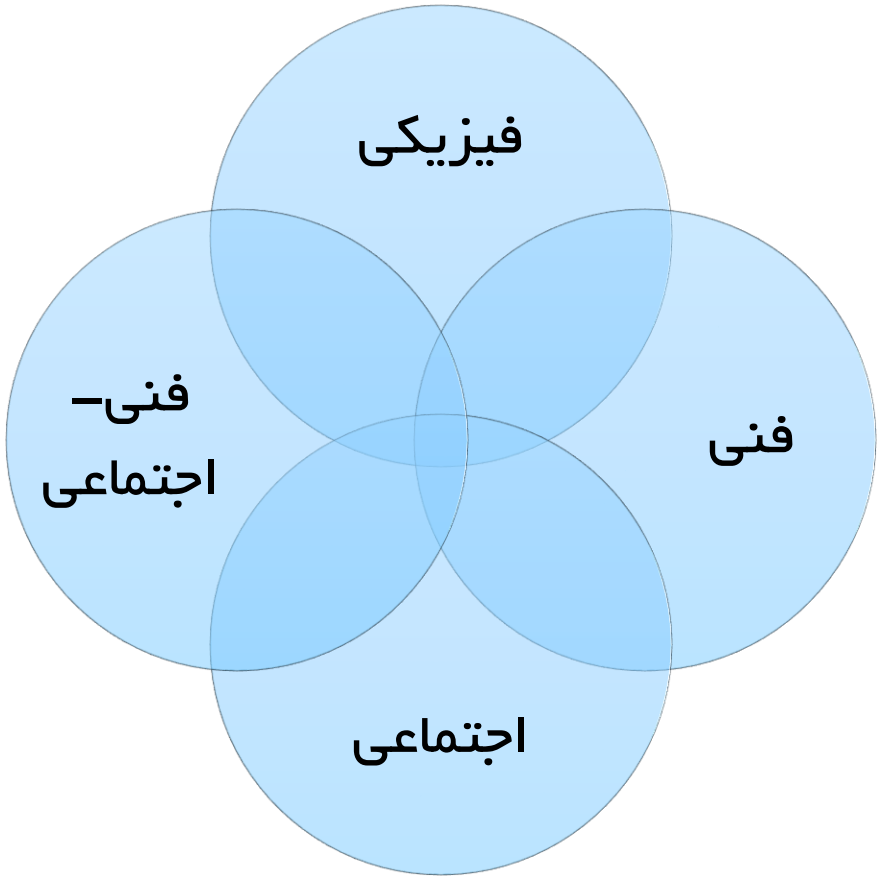
- محافظت در برابر بد افزارها
- مراقبت از ایمیل های آلود
- محافظت در برابر حملات مرورگر
- افزایش امنیت حساب های کاربری
- افزایش موفقیت برنامه های امنیت با کسب مهارت امنیتی

شگردهای تهدید امنیت اطلاعات در سازمان از سمت کارکنان

۱

ممکن است برای شما هم اتفاق بیافتد!

مهندسی اجتماعی



مهندسی اجتماعی Social Engineering **در حوزه امنیت اطلاعات؛** هنر متقاعد ساختن فرد، با استفاده از شستشوی مغزی، برای انجام دادن کاری که امنیت را به خطر بیاندازد.

۲

انواع حملات مهندسی اجتماعی

روش‌های فیزیکی

- زباله گردی
- سرقت تجهیزات
- نفوذ

روش‌های اجتماعی

- استفاده از تکنیک های روانشناسی برای شستشوی مغزی
- قدرت ادعایی
- تحریک کنجکاوی
- جبران لطف
- طعمه گذاری (فیشینگ، ایمیل آلوده و ..)

۲

انواع حملات مهندسی اجتماعی

مهندسی اجتماعی معکوس

- خرابکاری عمدی، تبلیغ و کمک رسانی

روش‌های فنی

- پیداکردن رمز عبور یکسان و ضعیف
- پیداکردن اطلاعات شخصی قربانیان

روش‌های فنی – اجتماعی

- ترکیبی از روش‌های قبل
- طعمه گذاری فلش آلوده
- ارسال ایمیل با عناوین محرمانه، کارمندان اخراجی
- ارسال لینک **فیشینگ از طرف سایر دوستان**

۲

ممکن است برای شما هم اتفاق بیافتد!

کلیپ 1

۲

5 هدفی هکر در مهندسی اجتماعی به دنبال آنها است

1. به دست آوردن نام کاربری و گذرواژه (پسورد)
2. گرفتن تاییدیه اجتماعی (تایید مهاجم توسط قربانی) یا معرفی و تایید مهاجم از سایرکارکنان سازمان.
3. انتقال یک فایل مخرب به یکی از کامپیوترهای سازمان بوسیله حافظه جانبی
4. انتقال یک فایل مخرب به یکی از کامپیوترهای سازمان بوسیله باز کردن یک فایل ضمیمه ایمیلی آلوده
5. گرفتن اسرار محرمانه در گفتگویی که ظاهراً با "همکار" انجام می‌شود (یعنی مهاجم هویت همکار را جعل کرده است).

۲

فیشینگ

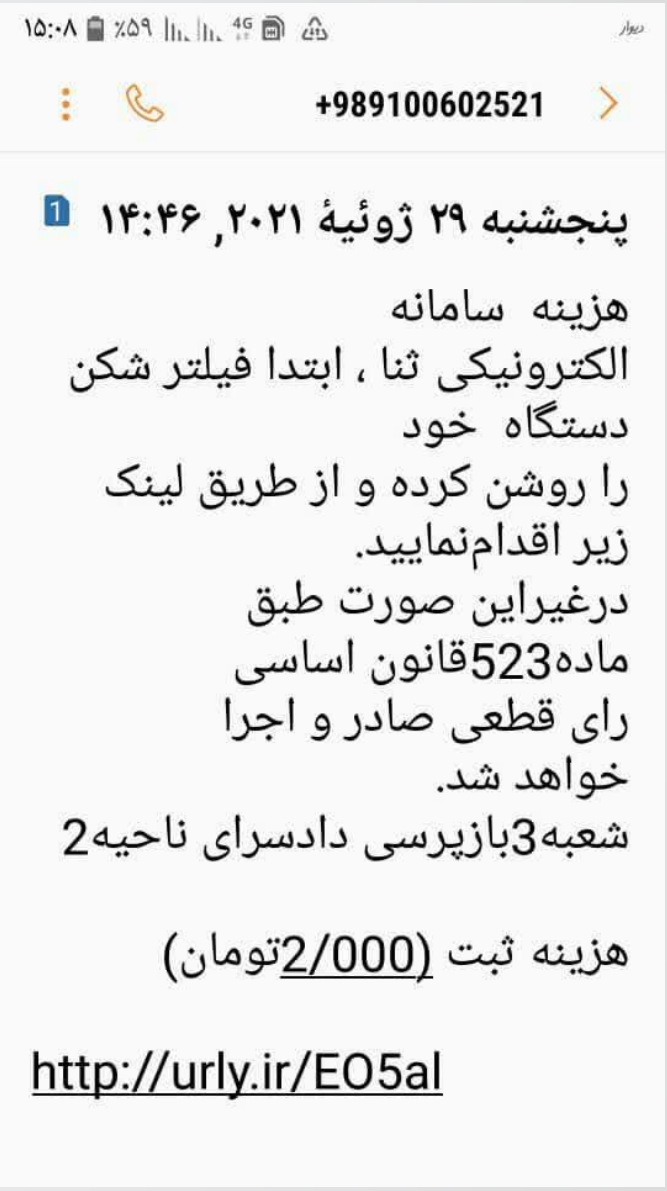
استفاده از پیامک

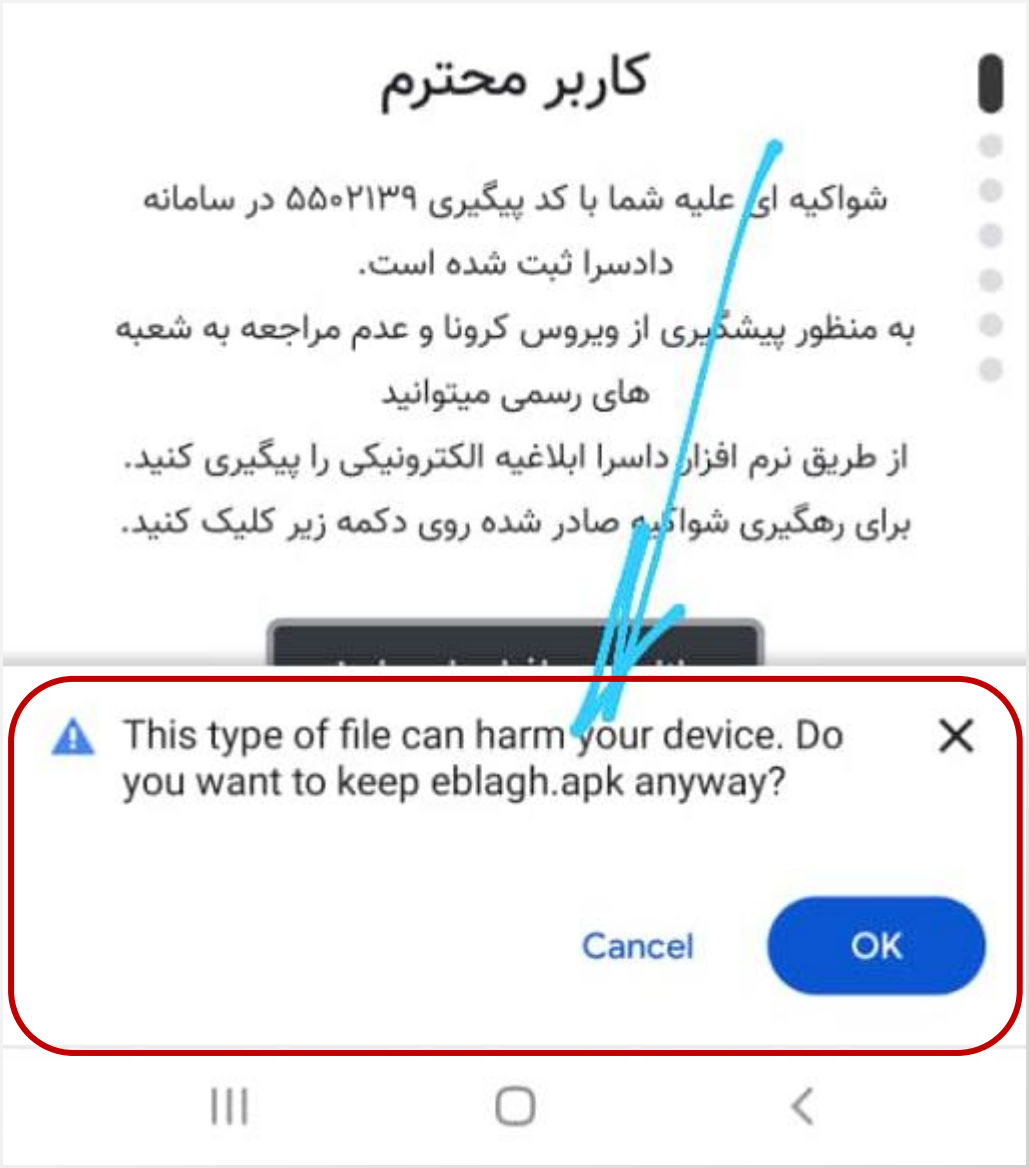
یـارانه شماقطع شدبرای فعال سازی در لینک زیر ثبت نام کنید.
yaranehe.com

کاربرگرامی اطلاعات حساب بانکی شما دچار مشکل شده است، شما باید نزد بانک مرکزی احراز هویت کنید. برای ثبت اطلاعات و احراز جهت جلوگیری از مسدود شدن حسابتان اطلاعات کارت بانکی خود بهمراه رمز دوم و شماره ملی خود به ایمیل بانک مرکزی به ادرس ufehy@hi2.in بفرستید.
باتشکر


مراقب پیامک‌های جعلی تحت عنوان سامانه ثنا باشید
مجرمان سایبری با ساخت آدرس اینترنتی جعلی به عنوان سامانه ثبت‌نام الکترونیک قوه قضاییه (ثنا) و ارسال پیامک‌های ساختگی با موضوعاتی از قبیل ابلاغیه، ثبت شکایت در سامانه و ... کاربران را به درگاه‌های جعلی هدایت می‌کنند.
CYBERPOLICE.IR
پلیس فضای تولید و تبادل اطلاعات ناجا


09331338678
(ابلاغ الکترونیک قضایی)
بنابرشکایتی که علیه شما صورت گرفته و درسایت ثبت شده است برای مشاهده از شکایت خود به سایت زیرمراجعه کنید درغیر این صورت طی(۲۴ ساعت) پرونده به دادگستری ارجاع خواهد شد.
شماره پرونده:
۹۸۳۵۱۱۰۰۳۱۶
آدرس پیگیری : sana-adliran.co/Eblagh/kap018ma91


+989100602521
پنجشنبه ۲۹ ژوئیهٔ ۲۰۲۱, ۱۴:۴۶
هزینه سامانه
الکترونیکی ثنا ، ابتدا فیلتر شکن
دستگاه خود
را روشن کرده و از طریق لینک
زیر اقدام‌نمایید.
درغیراین صورت طبق
ماده523قانون اساسی
رای قطعی صادر و اجرا
خواهد شد.
شعبه3بازپرسی دادسرای ناحیه2
هزینه ثبت (2/000تومان)
http://urly.ir/EO5al



ترغیب کاربر به نصب بدافزار

با نصب یک بدافزار که در پوشش یک برنامه کاربردی به کاربر معرفی می شود هکر به سادگی می تواند اطلاعات مهم کاربر را سرقت کند.

گاهی اوقات افراد بدون فکر محتواهای خـود را منتشـر می‌کنند.

یکـی از وظـایف مـا در قبـال سـازمان، مراقبـت در تمـام زمینه ها است.

کلیپ 2

۳

وبـسایت و شبکه‌های اجتماعی

اطلاعات وبـسایت سازمان یا شبکه‌های اجتماعی کارکنان جایگاه مناسبی برای جمع‌آوری اطلاعات!!

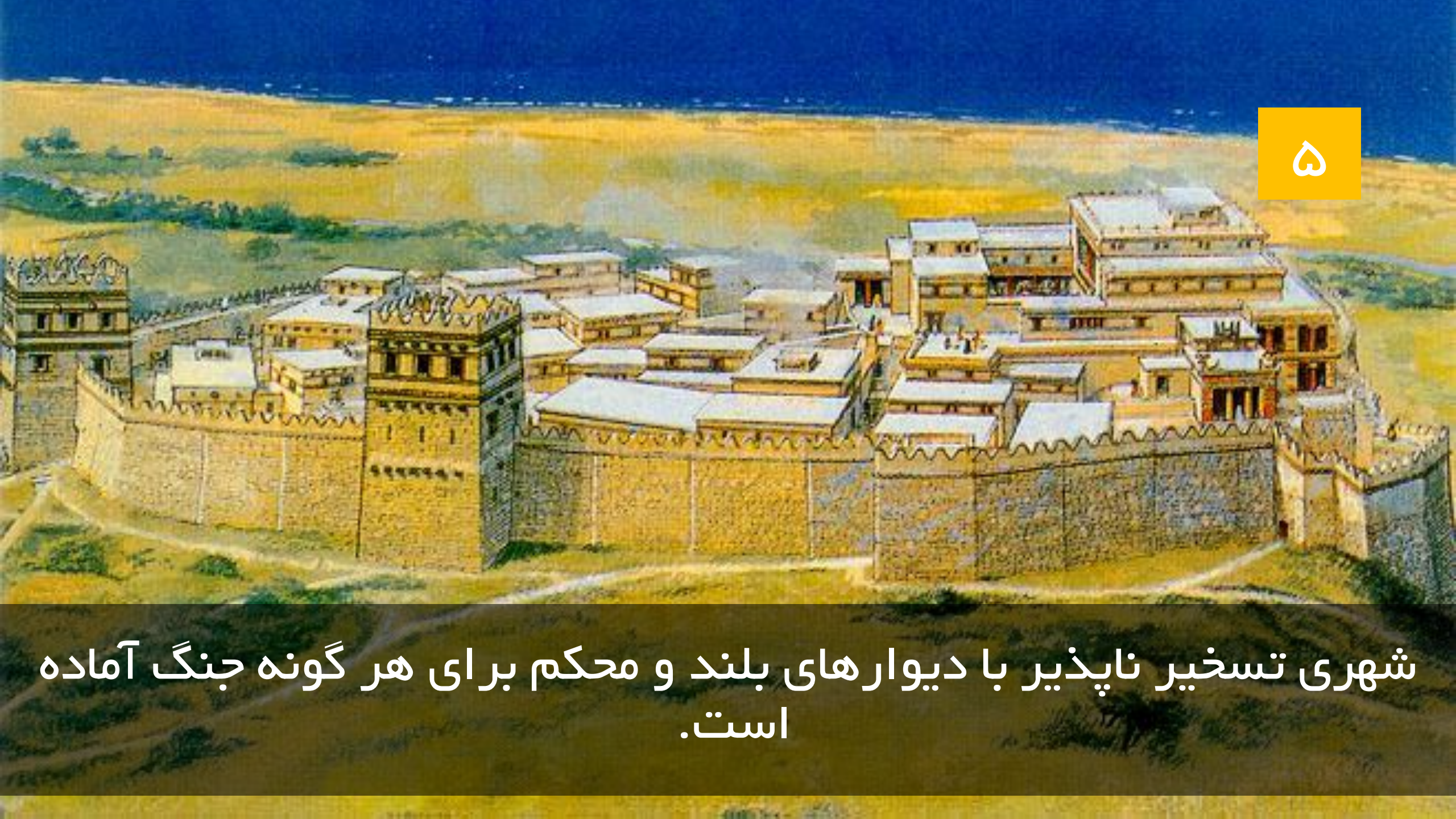
۴

استفاده از تجهیزات الکترونیک در سازمان فرصت یا تهدید؟

آیا می‌دانستید تمام تجهیزات الکترونیکی قابل نفوذ هستند!!!

همیشه مجازی نیست!

همیشه نباید حملات سایبری به صورت کاملاً مجازی انجام شود. در بیشتر موارد این نوع حملات و یا نفوذ به صورت ترکیبی از فضای مجازی و حقیقی انجام می‌شود.



۵

شهری تسخیر ناپذیر با دیوارهای بلند و محکم برای هر گونه جنگ آماده است.


اسب تروا قدیمی‌ترین
مهندسی اجتماعی دنیا

ویروس، تروجان و باج‌افزار در کمین

هر ۱۱ ثانیه یک حمله باج افزاری اتفاق می افتد و خسارت پیش بینی شده در پایان سال ۲۰۲۰ بالغ **بر ۲۰ میلیارد دلار** می باشد.

گزارش کمپانی Chainalysisکه یک موسسه پژوهشی بلاکچین است نشان می دهد که باندهای باج افزاری در سال ۲۰۲۰ حداقل **۳۵۰ میلیون دلار** از قربانیان خود باج دریافت کرده اند، این رقم نسبت به سال ۲۰۱۹ **رشدی ۳۱۱ درصدی** داشته است.