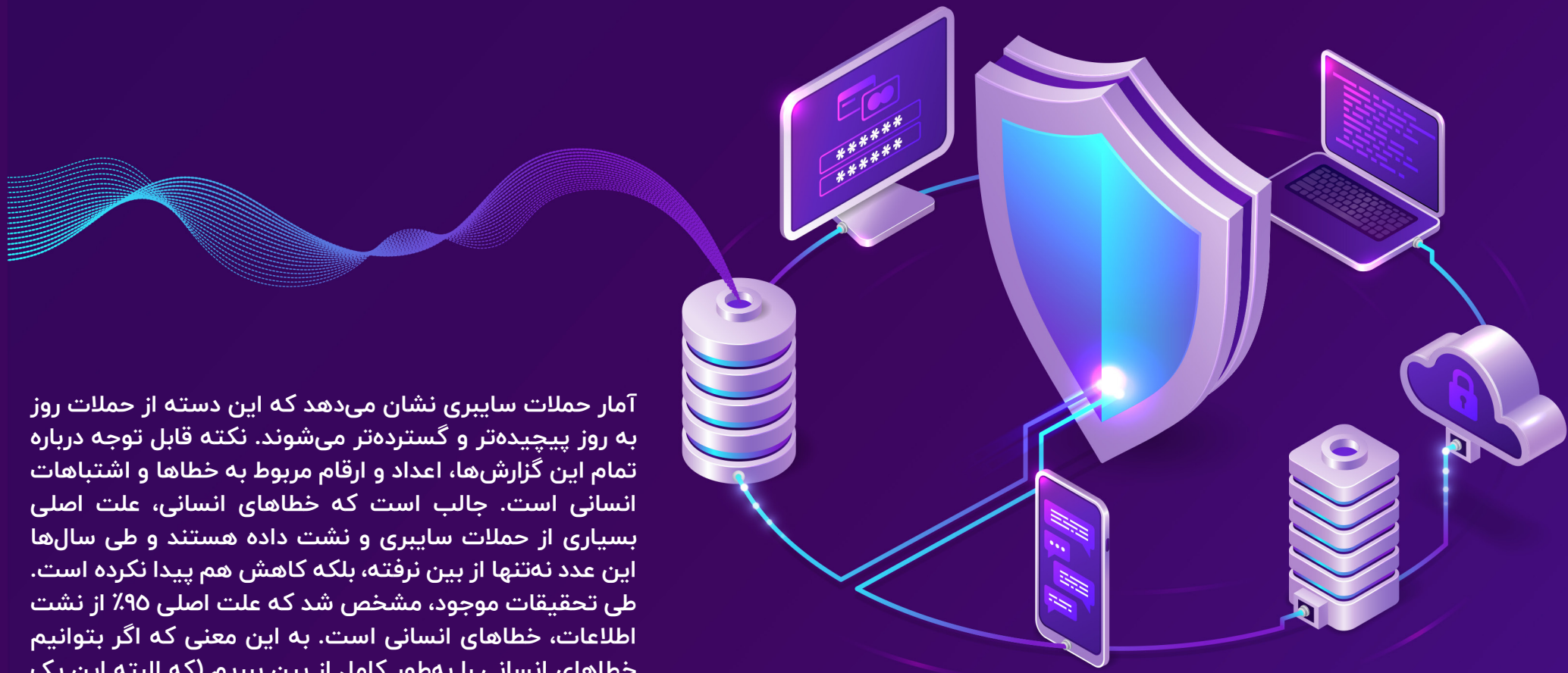
طرح وبینار رایگان امنیت سایبری
برای کارمندان سازمانی



آمار حملات سایبری نشان می‌دهد که این دسته از حملات روز به روز پیچیده‌تر و گسترده‌تر می‌شوند. نکته قابل توجه درباره تمام این گزارش‌ها، اعداد و ارقام مربوط به خطاها و اشتباهات انسانی است. جالب است که خطاهای انسانی، علت اصلی بسیاری از حملات سایبری و نشت داده هستند و طی سال‌ها این عدد نه‌تنها از بین نرفته، بلکه کاهش هم پیدا نکرده است. طی تحقیقات موجود، مشخص شد که علت اصلی ۹۵٪ از نشت اطلاعات، خطاهای انسانی است. به این معنی که اگر بتوانیم خطاهای انسانی را به‌طور کامل از بین ببریم (که البته این یک فرض محال است!)، از هر ۲۰ مورد نشت اطلاعات، ۱۹ مورد از آن‌ها اتفاق نمی‌افتد.

حتی شرکت‌های بزرگ هم از خطاهای انسانی در امان نیستند. برای مثال، در سال ۲۰۲۰ شاهد حمله فیشینگ به شرکت توئیتر بودیم که علت اصلی آن، سهل‌انگاری کارمندان توئیتر بود. در ادامه، چند مورد از آمار مربوط به خطاهای انسانی را آورده‌ایم:

۱. تقریبا نیمی از کارمندان سازمانی به وای‌فای عمومی اعتماد می‌کنند.

۲. ۱۴ درصد از کارمندان سازمانی تلفن‌های هوشمند خود را قفل نمی‌کنند.

۳. نیمی از کارمندان به خانواده یا دوستان خود، اجازه دسترسی به دستگاه‌های شرکتی را می‌دهند.

۴. خطای انسانی علت اصلی نشت اطلاعات است.

۵. طبق گزارش ۵۸٪ از سازمان‌ها، کارمندان از پیروی از دستورالعمل‌های امنیتی سر باز می‌زنند.

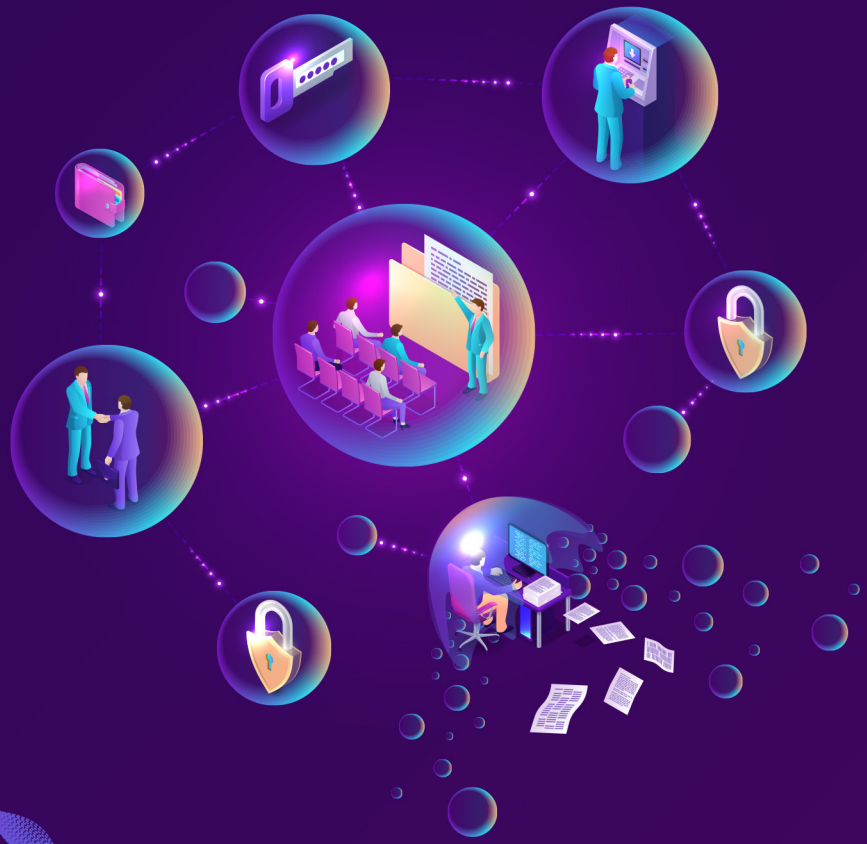
۶. اکثر افراد از رمزعبورهای ضعیف استفاده می‌کنند.

۷. استفاده مجدد از پسوردها بسیار رایج است.

۸. اشتراک‌گذاری پسورد بین افراد بسیار رایج است.

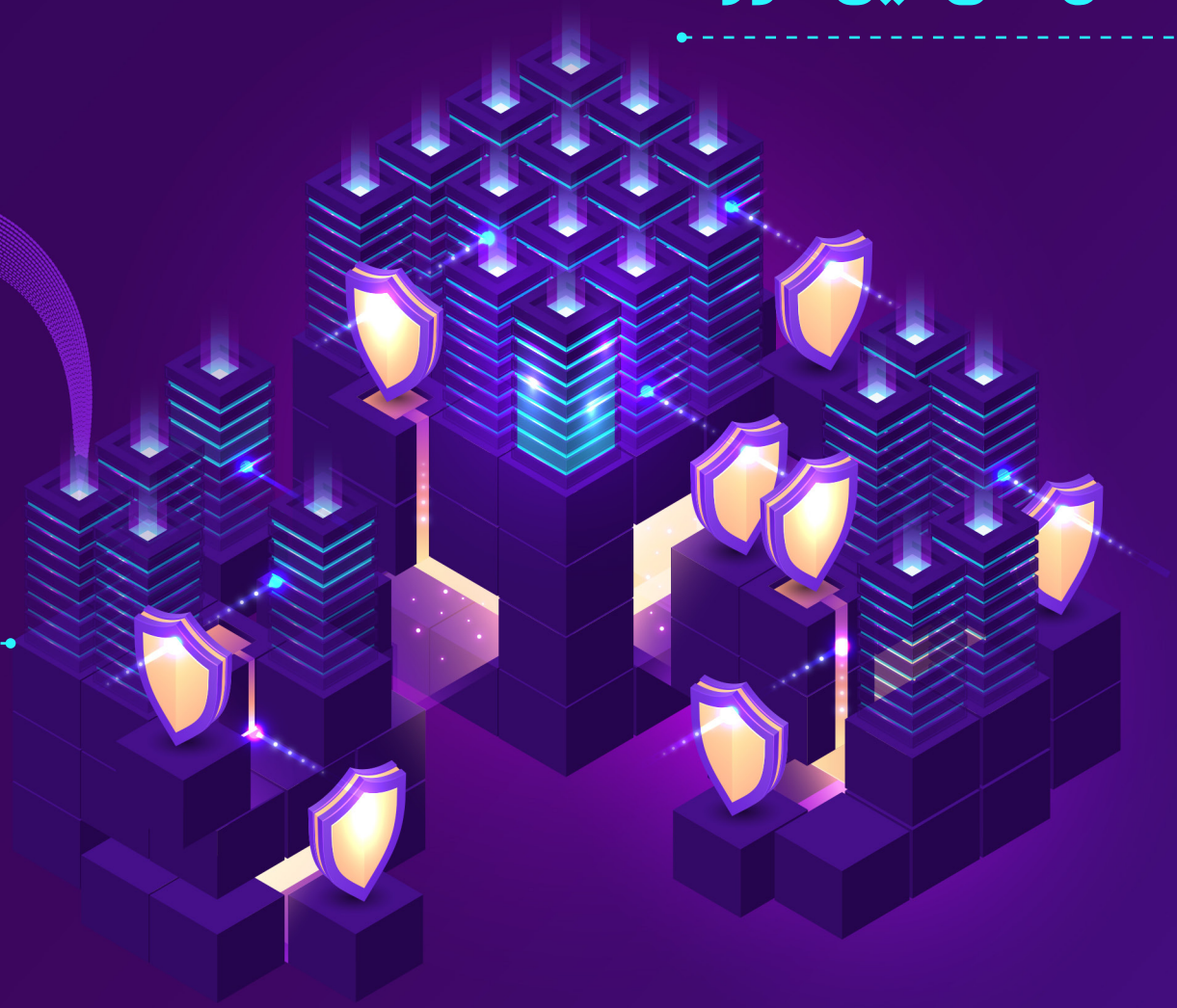
۹. تنها ۴۵٪ از افراد بعد از نشت اطلاعات، رمزعبور خود را تغییر می‌دهند.

۱۰. حدود ۵۰٪ از افراد، رمزعبور خود را روی کاغذی نوشته و به مانیتور می‌چسبانند.



همه این‌ها، نشان می‌دهد که سطح آگاهی کارمندان در حوزه امنیت تا چه اندازه کم است. این آگاهی در کشور ما پایین‌تر نیز هست؛ چراکه به دلیل عدم انتشار آمار حملات سایبری و نشت اطلاعات، بسیاری از شرکت‌ها آموزش‌های امنیتی کارکنان خود را جدی نمی‌گیرند و با این توجیه که هکرها شرکت‌های کوچک را هدف قرار نمی‌دهند، از زیر بار این مسئولیت شانه خالی می‌کنند.
برای رد این توجیه اشتباه، کافی است نگاهی به گزارش سالیانه نشت اطلاعات بیاندازید و ببینید که مهاجمان تا چه حد به سازمان‌های کوچک و متوسط علاقمند هستند. این موضوع می‌تواند برای شرکت‌ها و سازمان‌ها خطرآفرین باشد زیرا تمام سرمایه و اعتبار آن‌ها ممکن است با یک اشتباه پرسنل از بین برود. بنابراین منطقی است که روی آموزش پرسنل خود سرمایه‌گذاری کنند تا بتوانند ریسک حمله و نشت اطلاعات ناشی از آن را به میزان چشمگیری کاهش دهند.
پرسنل شما باید از خطراتی که تهدیدشان می‌کند، آگاه باشند و بتوانند در زمان مناسب، تصمیم درستی بگیرند. در دوره «مبانی امنیت سایبری» که توسط گروه لیان و با هدف آموزش پرسنل عادی طراحی شده است، کارمندان شما با مفاهیم اولیه حملات سایبری آشنا می‌شوند و مکانیزم وقوع یک حمله را می‌شناسند.
مهم‌ترین بخش این دوره، آموزش راهکارهای امنیتی جهت بالابردن امنیت فرد و سازمان است. ما سعی می‌کنیم با معرفی شیوه‌های مختلف حملات سایبری، به دانشجویان بیاموزیم که چگونه قربانی این حملات نشوند و اگر قربانی شدند، چه اقدامات امنیتی برای مقابله یا جلوگیری از وارد شدن خسارات بیشتر انجام دهند.

سرفصل‌های این دوره:



- مفاهیم ابتدایی امنیت سایبری
- فرایندهای بنیادی حوزه امنیت
- امنیت در سیستم عامل
- تهدیدات رایج در سیستم عامل‌ها
- نحوه انتشار بدافزارها