جلسه دوم

پیشگیری از تهدیدهای امنیت اطلاعات

راه کارها و توصیه های کاربردی

۱

پیشگیری از مهندسی اجتماعی

- شناخت تکنیک های مهندسان اجتماعی که از احساسات انسانی، مانند کنجکاوی یا ترس برای فریب قربانیان خود استفاده می کنند.
- محتاط بودن در مواجهه با تبلیغات و ادعاهای مطرح در شبکه های اجتماعی و ایمیل.
- به روز بودن در برابر شگردهای جدید مجرمانه.

۱ توصیه های کاربردی برای پیشگیری از مهندسی اجتماعی

ایمیل و پیوست ها را از منابع مشکوک باز نکنید

- اگر فرستنده ایمیل را نمی شناسید ، نیازی به پاسخ دادن به ایمیل نیست.
- حتی اگر فرستنده را می شناسید ولی در مورد پیام مشکوک هستید ، اخبار را از منابع دیگر مانند تلفن یا مستقیماً از سایت ارائه دهنده خدمات بررسی کرده و تأیید کنید.
- به یاد داشته باشید که آدرس های ایمیل همیشه جعل می شوند. حتی ایمیلی که گویا از یک منبع معتبر می آید ممکن است در واقع توسط یک مهاجم ایجاد شده باشد.

ایمیل و پیوست ها را از منابع مشکوک باز نکنید

Forwarded

Dear Sir/Madam,

This ticket is sent you by Cyber Police of the I.R of Iran. We are investigating about internet fraud in our country, which the criminal person has exchanged some money from victim (kavirdashtetoos@gmail.com). You are kindly requested to provide us with the information (Login IPs, Transactions, Destinations, ...) of the below mentioned accounts and send the information for us to fata@police.ir.
Thanks in advance,

myboxmail007@gmail.com
paloppper@gmail.com

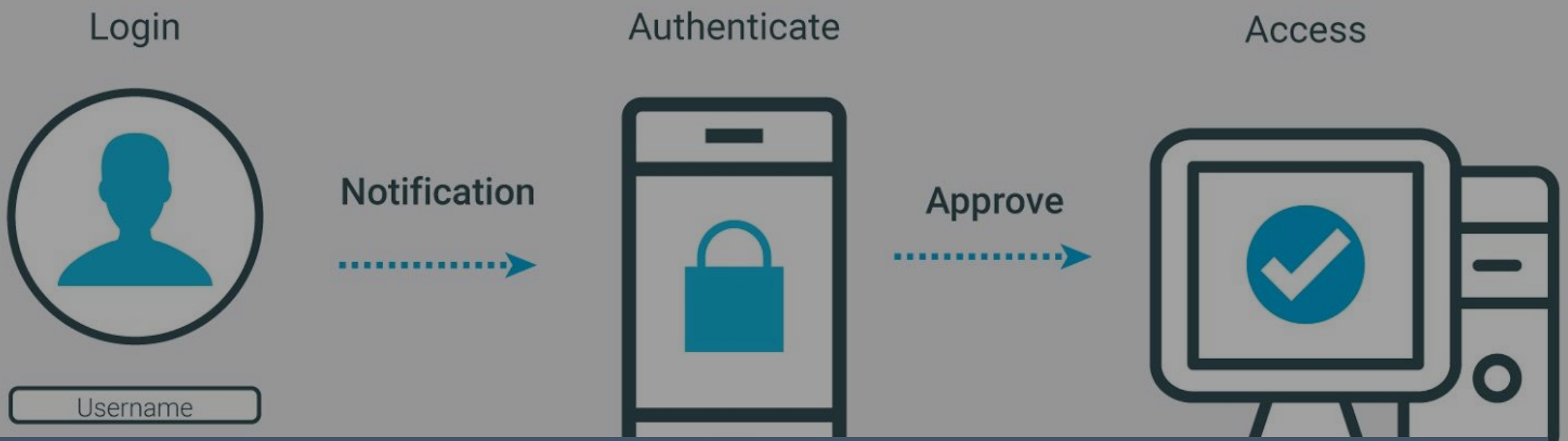
Best Regards,
Cyber Police of the I. R of Iran
Tel: +982188878385
Email: fata@police.ir
www.cyber.police.ir

15:00

ایمیل ها همیشه از آنجاییکه ادعا می کنند نمی آیند.

۱ توصیه های کاربردی برای پیشگیری از مهندسی اجتماعی

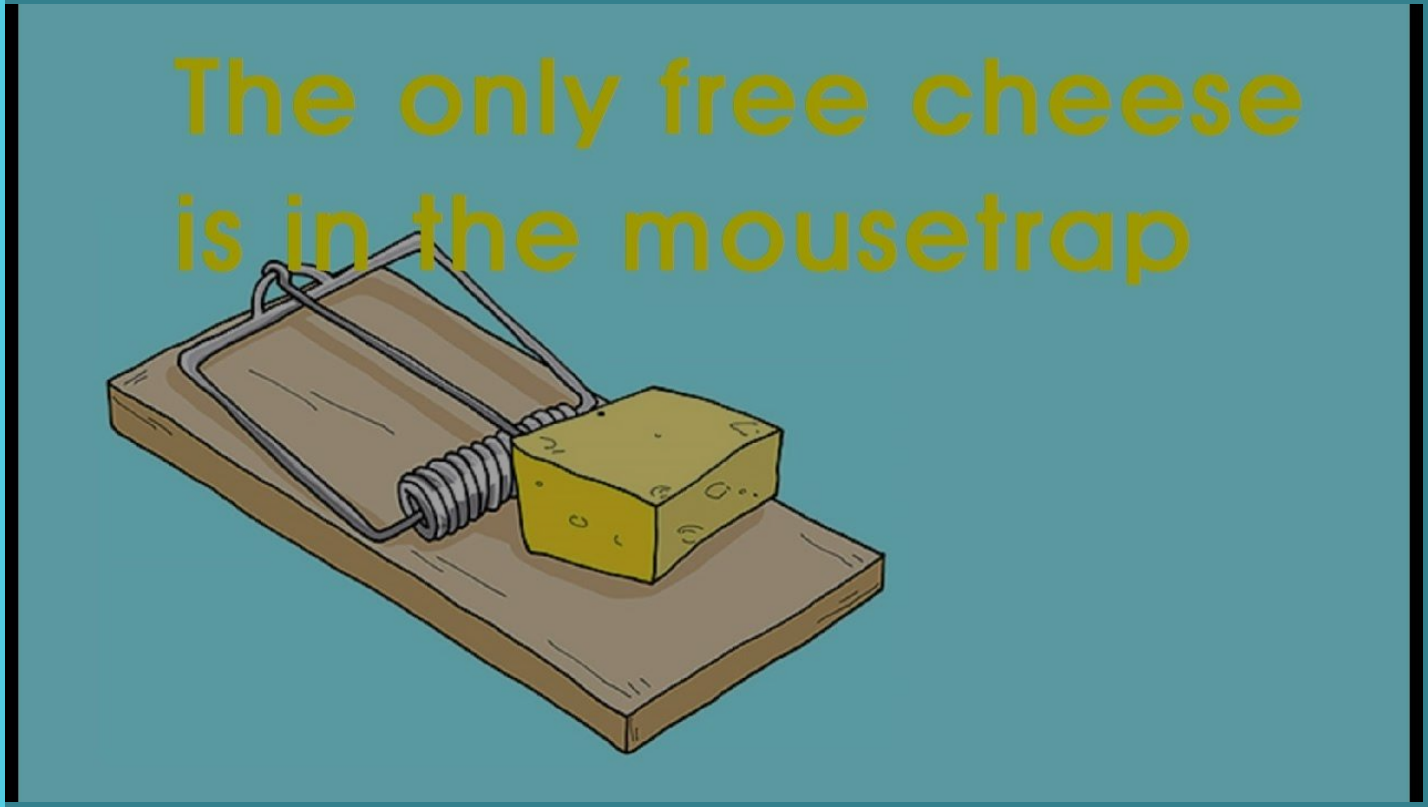
از احراز هویت چند عاملی استفاده کنید



یکی از با ارزش ترین اطلاعاتی که مهاجمان به دنبال آن هستند اعتبار کاربر است. استفاده از احراز هویت چند عاملی به شما کمک می کند تا در صورت به خطر افتادن سیستم از محافظت از حساب خود اطمینان حاصل کنید.

۱ توصیه های کاربردی برای پیشگیری از مهندسی اجتماعی

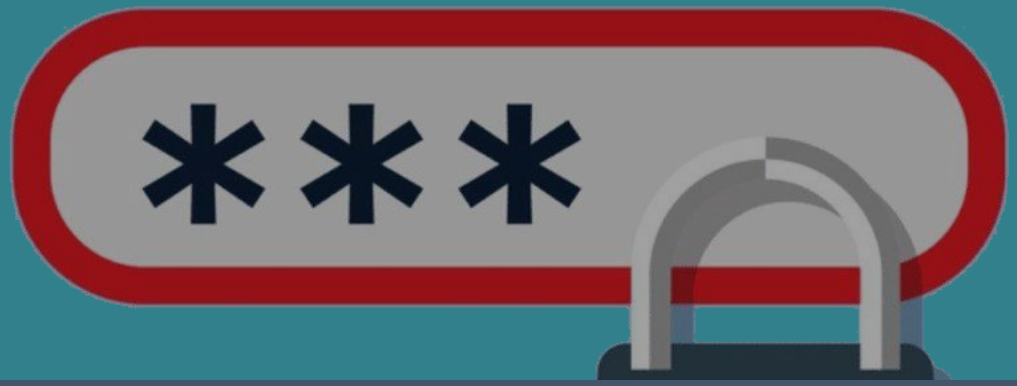
مراقب پیشنهادهای وسوسه انگیز باشید.



- اگر پیشنهادی بیش از حد فریبنده به نظر می رسد ، قبل از پذیرفتن آن خوب فکر کنید. جستجو در مورد موضوع می تواند به شما کمک کند تا به سرعت تشخیص دهید که با یک پیشنهاد قانونی روبرو هستید یا یک دام.
- اگر احساس کردید فردی یا یکی از همکاران برای کسب اطلاعات از شما سماجت می کند بیشتر مراقب باشید.

۱ توصیه های کاربردی برای پیشگیری از مهندسی اجتماعی

از رمزهای عبور قوی و یک برنامه مدیریت رمز عبور استفاده کنید.



- هر یک از رمزهای عبور شما باید منحصر به فرد و پیچیده باشد.
- کلمه عبور حداقل 10 کاراکتر متشکل از انواع کاراکتر های متنوع ، از جمله حروف بزرگ ، اعداد و نمادها باشد.
- رمزهای عبور خود را به صورت دوره ای تغییر دهید.
- برای کمک به مدیریت همه گذرواژه های خود می توانید از یک برنامه مدیریت گذرواژه استفاده کنید.

How to

CREATE A STRONG PASSWORD

Don't use:

COMMON WORDS ⊘ names or 'password'

TRICKY COMMON CHARACTER SUBSTITUTIONS ⊘ p@55w0rd

Sequences

- NEIGHBORING KEYSTROKES ⊘ qwerty
- REPEATED CHARACTERS ⊘ aaaaaaa
- CHARACTER SEQUENCE ⊘ abcdefg
- NUMBER ⊘ 15783

BIRTH YEAR ⊘ 1989

COMPLETE DATE ⊘ 01261987

کلمه عبور قوی بسازید

- از این عبارات استفاده نکنید:

1- کلمات عمومی مانند نام ، پسورد و ...

2- استفاده از کاراکترهای پرکاربرد جایگزین

3- کلمات کنار هم در صفحه کلید

4- تکرار کاراکتر

5- کاراکترهای رشته ای

6- اعداد

7- سال تولد

8- تاریخ تولد

تکنیک های تولید کلمه عبور و به خاطر سپاری آن

روش	کلمه عبور قوی	جمله پایه
استفاده از حروف بزرگ و کوچک	God Is My Only Hope.	God is my only hope.
جایگزینی کاراکترها با نشانه و عدد	G0d1sMy0n!yHope.	God is my only hope.
تغییر زبان صفحه کلید	"Onh jkih hldn lk hsj"	"خدا تنها امید من است"
خلاصه نویسی با علائم اختصاری	"rU:-)2d@y"	"Are you happy today"

راهکارهای مدیریت کلمه عبور

بسیاری از کاربران کلمات عبور خود را در مرورگر ذخیره می کنند این کار می تواند خطراتی به دنبال داشته باشد.

از دست رفتن کلمات عبور با تعویض سیستم عامل

دسترسی هکر به کلمه عبور در صورت دسترسی به رایانه

عدم مدیریت پیچیدگی کلمه عبور و به خاطر سپاری

به جز فایرفاکس بقیه مرورگرها Master password ندارند

برنامه های مدیریت کلمه عبور

- برنامه های مدیریت کلمه عبور راهکاری ساده امن برای حفظ هویت در فضای مجازی

برنامه های مدیریت کلمه عبور

Dashlane: #1
Password Manager

F-Secure KEY Password
manager

1Password -
Password Manager

Password Manager

My Passwords

Keeper®: Free Password
Manager

Avast Passwords

Hide Pictures
Keep Safe Vault

LastPass Password
Manager

سرقت کلمه عبور با کیلاگر

Hardware Keylogger

نبایدها

نباید اطلاعات کاری شما را با دوستان خود به اشتراک بگذارند.

نباید با استفاده از گوشی و تجهیزات شما به شبکه‌های اجتماعی و یا حساب‌های کاربری خود وارد شوند.

شما **نباید** اطلاعات ورود به حساب‌های کاربری و کاری خود را در اختیار آنان قرار دهید.

اعضای خانواده و افراد نزدیک شما **نباید** بدون اطلاع شما اطلاعات شما را در اختیار دیگران قرار بدهند.

نباید بدون احراز هویت کامل و تنها کفایت به کاربری شبکه‌های اجتماعی به یکدیگر اعتماد کنید.

۲

خانواده و افراد نزدیک کارمند هدف

دسترسی به اطلاعات حساس سازمان از طریق ارتباط با خانواده مدیرعامل یا مدیر خدمات

۲

نظر شما چیست؟

کلیپ 4

۲ از خودتان داده منتشر نکنید

از به اشتراک گذاری نام مدارس ، دوستان، اعضاء خانواده، محل تولد یا سایر مشخصات شخصی خود خودداری کنید.

شما ممکن است به طور ناآگاهانه پاسخ سوالات امنیتی یا بخشهایی از رمز ورود خود را در معرض دید قرار دهید. اگر سوالات امنیتی خود را طوری تنظیم کنید که به یادماندنی اما نادرست باشند ، شکستن حساب شما برای یک هکر سخت تر می شود. مثلا اگر اولین اتومبیل شما "تویوتا" بود ، نوشتن نام دروغینی مانند "ماشین دلقک" می تواند هکرهای کنجکاو را کاملاً دور بیندازد.

۳

ویروس، تروجان و باج‌افزار در کمین

پیشگیری بهتر از درمان

راهکارهای مقابله

- نصب آنتی ویروس اورجینال و به روز نگه داشتن آن
- تهیه نسخه پشتیبان بصورت مداوم از اطلاعات
- به روز نگه داشتن سیستم عامل
- استفاده از ابزارهای اختصاصی مانند Anti-Malwareها
- به محض تشخیص آلوده شدن سیستم: قطع هرگونه ارتباط با اینترنت و شبکه
- عدم کلیک بر روی لینک های مشکوک

۴

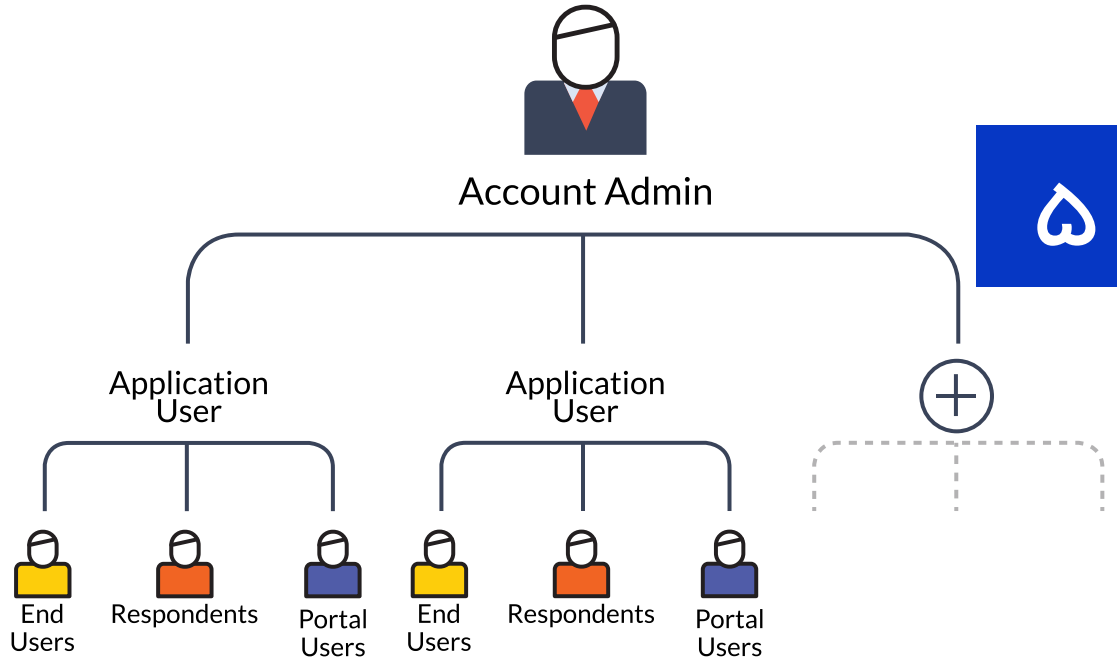
اهمیت پشتیبان‌گیری از داده‌ها

ارزش پشتیبان بیش از داده‌ی اصلی!

حملات سایبری و ransomware تنها تهدیدات برای داده‌های سازمان نیستند. این داده‌ها ممکن است حتی با بلاهای طبیعی از بین روند. از این رو پشتیبان‌گیری در فرمت و نسخه‌های مختلف برای سازمان ضروری است.

دستورالعمل های نگهداری و پشتیبان گیری از داده را رعایت کنید

۵



یکـی از مهمتـرین مـواردی کـه تمـامی پرسـنل

سازمان از جمله مدیران **باید** به آن عمل کننـد

حفـظ اطلاعـات کـاربری و رعایـت نکـات حفـاظتی

می‌باشد. همچنین علاوه بر رعایت سطح دسترسی

کارکنـان، **حفـظ دسترسـی بـه**

اطلاعات بسیار اهمیت دارد.

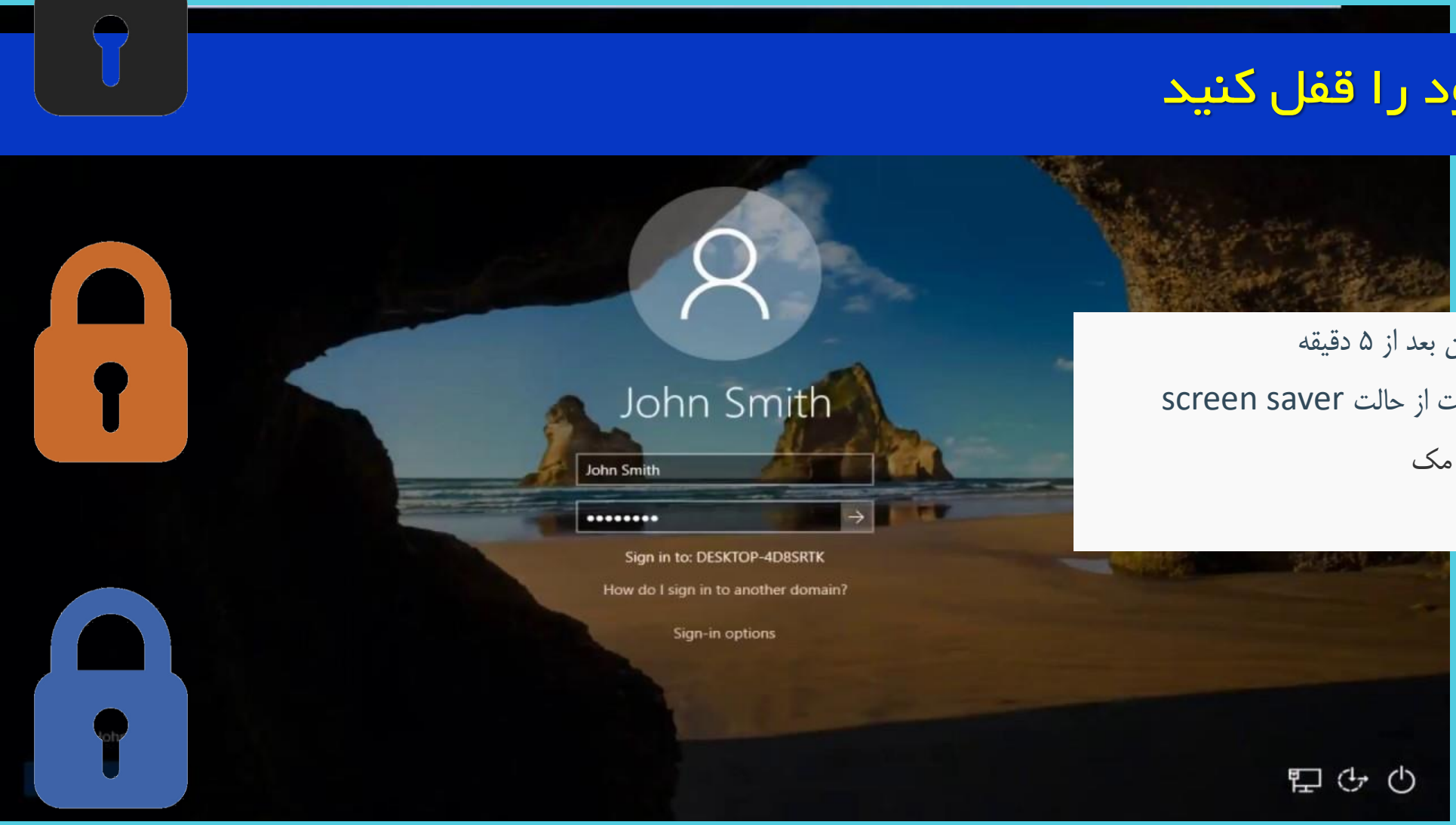
رعایت سطح دسترسی در مجموعه و حفظ اطلاعات

هیچگاه دسترسی خود را در اختیار دیگران قرار ندهید.

ارزش اطلاعات کارکنان یک سازمان کمتر از ارزش اطلاعات آن سازمان نیست!

۶

صفحه نمایش خود را قفل کنید



- فعال شدن screen saver شدن بعد از ۵ دقیقه
- فعال کردن کلمه عبور برای بازگشت از حالت screen saver
- Control+Shift+Power در مک
- windows+L در ویندوز

۷

در مواجهه با این موارد هوشیار باشید

- گزارش وضعیت نرم افزارهای به روز نشده به مسئولین مربوطه.
- ذخیره سازی نادرست و غیراصولی بانک داده
- ارسال اشتباهی اطلاعات سازمان به دیگران را گزارش دهید
- مراقبت تجهیزات هوشمند قابل حمل تان باشید

یادمان باشد که:

هیچ وصله‌ای برای غفلت انسان وجود ندارد.

پرسش و پاسخ

امنیت در فضای مجازی

به امید دیدار