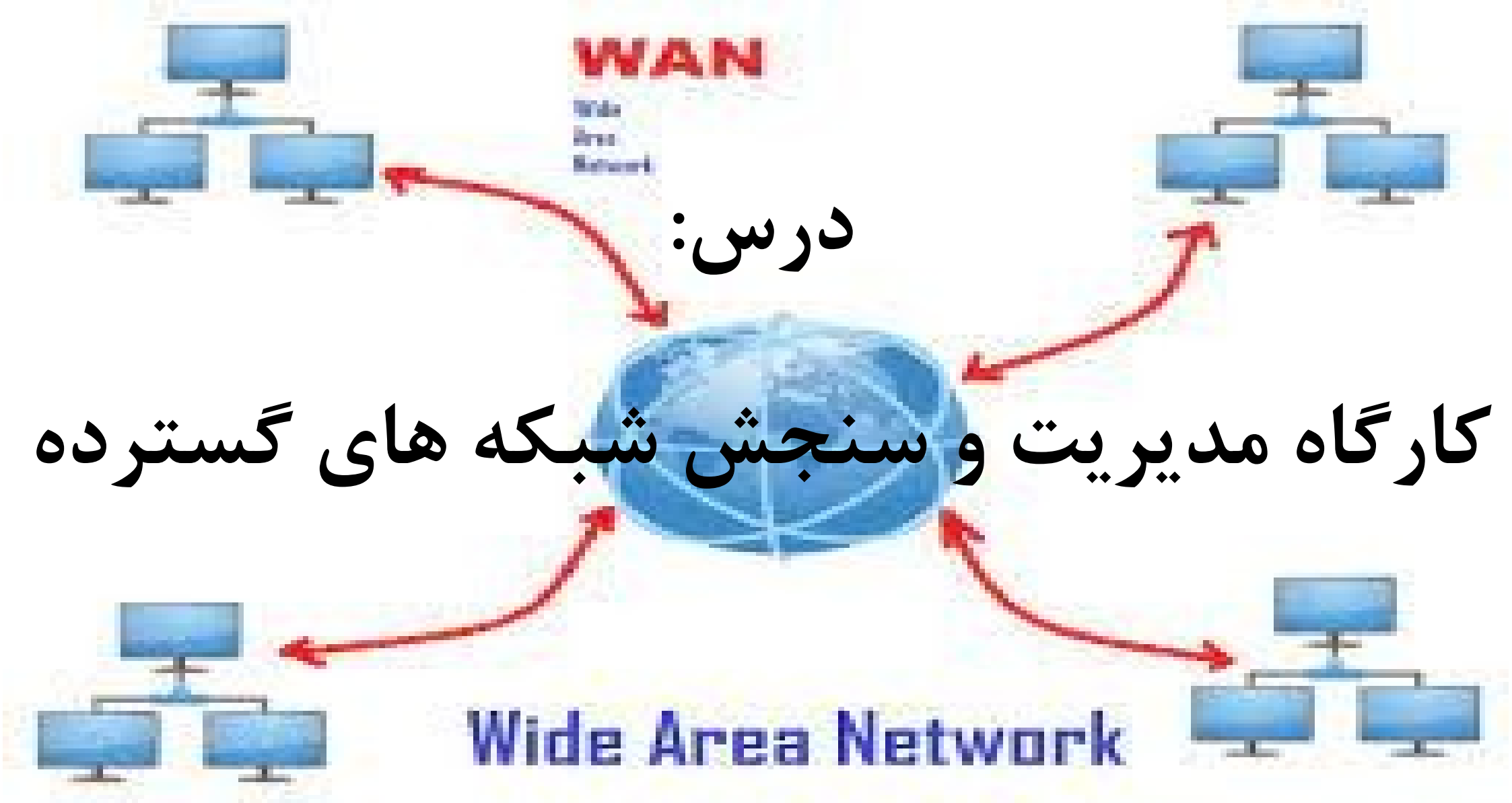
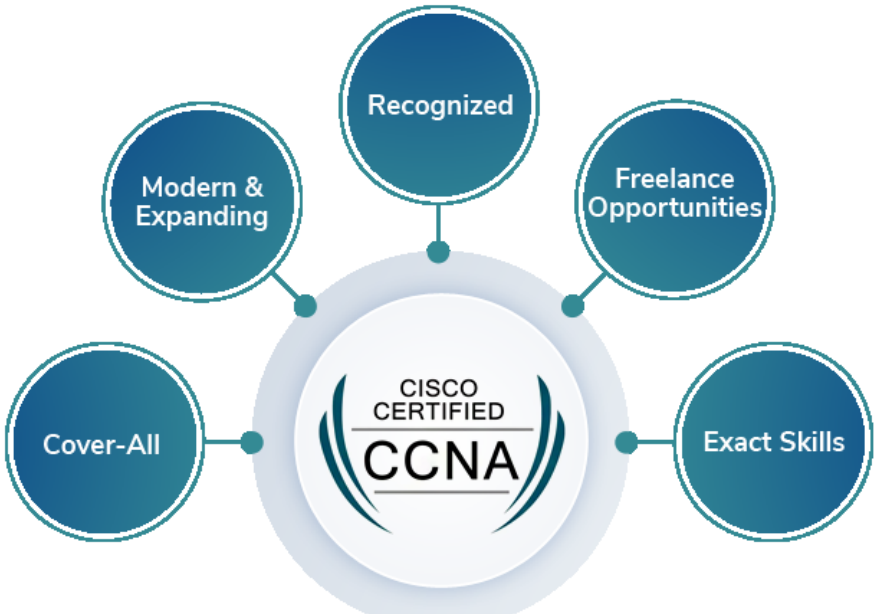



درس:

# کارگاه مدیریت و سنجش شبکه های گسترده

## مدرس: اسماعیل طغرایی

ایمیل: Toghraee_University@yahoo.com
وب سایت ها: https://Teach.toghraee.ir
https://Toghraee.ir




## دوره های تدریس:

- ✓ طراحی و پیاده سازی وب سایت HTML، PHP و...
- ✓ شبکه های کامپیوتری Network+
- ✓ دوره های CCNA و Intro
- ✓ برنامه نویسی C# و JS و Matlab
- ✓ طراحی و پیاده سازی وب سایت




## چگونه کلمه عبور مناسب بسازیم و از آن نگهداری کنیم؟

رمز عبور یا همان پسورد شما، کلیدی است که برای دسترسی به اطلاعات شخصی خود که در کامپیوتر و حساب های آنلاین ذخیره کرده اید، به کار می رود. .....

# چه عواملی یک پسورد را در مقابل حملات، قدرتمند می سازد؟

- یک پسورد قوی، باید به صورت رشته ای تصادفی از کاراکترها باشد. معیارهای زیر می تواند به این امر کمک کند:
- **طولانی بودن :**هر کاراکتری که شما به رمز عبور خود اضافه می کنید، حفاظت ایجاد شده به وسیله آن را چندین برابر افزایش می دهد. طول کلمه عبور شما باید 8 کاراکتر و یا بیشتر باشد. 14 کاراکتر یا بیشتر ایده آل است.
- **ترکیب حروف، اعداد و علائم :**هر چقدر تنوع کاراکترهایی که در رمز عبور استفاده می شود، بیش تر باشد، حدس زدن آن دشوارتر می گردد.
- سایر جزئیات مهم عبارتند از:
- هر چه تنوع کاراکترها کمتر باشد، پسورد باید طول بیشتری داشته باشد. اگر شما نمی توانید کلمه عبوری شامل علامت ها بسازید، نیاز دارید برای داشتن همان درجه از حفاظت، آن را به طور قابل ملاحظه ای طولانی تر کنید.
- از سرتاسر صفحه کلید (و نه فقط کاراکترهای رایج) استفاده کنید. سمبل هایی که با نگه داشتن دکمه "shift" و زدن یک عدد تایپ می شوند مانند @، #، % و ... در کلمات عبور بسیار مرسوم اند. در صورتی که از تمامی علامت های روی صفحه کلید از جمله علائم نقطه گذاری مانند ? ، ! ، " و ... استفاده شود، پسورد شما بسیار قوی تر خواهد شد.
- از کلمات و عبارت هایی که به یاد آوردن آن برای شما آسان است اما حدس زدن آن برای دیگران دشوار می باشد، استفاده کنید. ساده ترین راه برای به خاطر آوردن پسوردها و عبارات عبور، نوشتن آن ها بر روی کاغذ می باشد.
- بر خلاف باور عموم، نوشتن رمز عبور اصلا کار اشتباهی نیست، اما به منظور امن ماندن آن، باید به اندازه کافی محافظت شود. به طور کلی، رمز عبور نوشته شده بر روی یک تکه کاغذ، نسبت به رمز عبور ذخیره شده در وب سایت ها و دیگر ابزارهای نرم افزاری مانند نرم افزار مدیریت پسورد، در هنگام استفاده از اینترنت کم تر به خطر می افتد.

# ساختن یک پسورد قوی که بتوان به یاد آورد

راه های زیادی برای ساختن یک کلمه عبور طولانی و پیچیده وجود دارد. در این جا روشی معرفی می کنیم که یادآوری آن را نیز ساده می سازد.

| مثال | پیشنهاد | روش کار |
|---|---|---|
| Long and complex passwords are safest. I keep mine secret. | به چیزهایی که برای شما با معنی است فکر کنید. | با یک یا دو جمله در حدود 10 کلمه شروع کنید. |
| lacpasikms (10 characters) | از اولین حرف هر کلمه استفاده کنید. | جمله خود را به حروف پشت سر هم تبدیل کنید. |
| lACpAsIKMs (10 characters) | حروف نیمه اول الفبا را بزرگ کنید. | پیچیدگی را بیشتر کنید. |
| lACpAs56IKMs (12 characters) | یک عدد دو رقمی که برای شما معنی دارد را در بین دو جمله قرار دهید. | طول را با اعداد افزایش دهید. |
| ?lACpAs56IKMs (13 characters) | یک کاراکتر نقطه گذاری در ابتدا اضافه کنید. | طول را با علائم نقطه گذاری زیاد کنید. |
| ?lACpAs56IKMs@ (14 characters) | یک کاراکتر سمبل به انتها اضافه کنید. | طول را با سمبل ها افزایش دهید. |

پسورد جدید خود را با Password Checker تست کنید .

Password Checkerابرازی است که قدرت پسورد شما را به طور اتوماتیک، در حین تایپ کردن ارزیابی می کند. برای استفاده از آن روی لینک زیر کلیک کنید .

https://www.microsoft.com/protect/fraud/passwords/checker.aspx

## الگوهای خطرناک پسورد که باید از آن اجتناب شود

مجرمان سایبری از ابزارهای پیچیده ای که می تواند به سرعت رمزهای عبور را کشف کند، استفاده می کنند. برخی از روش های معمول مورد استفاده برای ایجاد کلمات عبور، به سادگی توسط هکرها حدس زده می شود. برای اجتناب از ایجاد پسوردهای ضغیف که به آسانی حدس زده می شود، باید از موارد زیر دوری کنید:

- **جملات و کاراکترهای تکراری**"12345678" :، "222222"، "abcdegf"و یا حروف کنار هم در صفحه کلید شما، کمکی به ساخت یک پسورد امن نمی کند.
- **استفاده تنها از جایگزینی حروف با اعداد و سمبل های مشابه :**تبهکاران و یا دیگر افراد خرابکار که به حد کافی برای شکستن رمز عبور شما آگاه هستند، با این جایگزینی های رایج مانند عوض کردن "i" با "1" و یا "a" با "@" به عنوان مثال در کلمات "M1cr0$0ft" و"P@ssw0rd" ، فریب نمی خورند. اما زمانی که این جایگزینی های با معیارهای دیگر مانند طول پسورد، غلط املایی و دگرگونی ساختار کلمه عبور و جابجایی اجزای آن، ترکیب شود، می تواند برای بهبود استحکام رمز عبور شما موثر باشد.
- **استفاده از نام کاربری خود :** هر قسمت از نام، تاریخ تولد و شماره شناسنامه شما و یا اطلاعات مشابه در مورد عزیزانتان، انتخاب بدی برای ساخت پسورد می باشد. آن ها یکی از اولین مواردی است که مجرمان امتحان می کنند.
- **کلمات موجود در فرهنگ لغت هر زبانی** :مجرمان از ابزارهای پیچیده ای استفاده می کنند که می تواند به سرعت پسوردهایی که بر اساس واژه های موجود در چندین فرهنگ لغت (شامل کلماتی که برعکس خوانده می شود، غلط های املایی و جایگزینی های متداول) ساخته می شود را حدس بزنند.
- **استفاده از یک رمز عبور در همه جا :**اگر هر کدام از کامپیوترها و یا سیستم های آنلاین که از این پسورد مشترک استفاده می کند به خطر بیفتد، باید در نظر گرفته شود که تمام اطلاعات دیگر شما که توسط این رمز حفاظت می شود نیز به خطر خواهد افتاد. این نکته بسیار حیاتی و حائز اهمیت است که برای سیستم های مختلف از کلمات عبور متفاوت استفاده شود.
- **سیستم های ذخیره سازی آنلاین** : اگر افراد خرابکار به این پسوردهای ذخیره شده در سیستم های آنلاین و یا روی یک کامپیوتر در شبکه مانند سرور، دسترسی پیدا کنند، آن گاه به همه اطلاعات شما دسترسی پیدا می کنند.

# 5.نکته برای این که پسورد خود را مخفی نگاه دارید

1. **هرگز رمز عبور خود را در یک ایمیل و یا بر اساس یک درخواست ایمیلی وارد نکنید .**هر ایمیلی که پسورد شما را درخواست می کند و یا از شما می خواهد که با مراجعه به یک وب سایت، رمز عبور خود را برای تصدیق صحت وارد کنید، اغلب تقلبی و برای فریب شما است. این شامل درخواست از شخص و یا شرکت مورد اعتماد نیز می باشد. محتویات پست الکترونیکی در حین انتقال می تواند خوانده شود و ایمیلی که درخواست اطلاعات می کند، ممکن است از طرف فرستنده ای که آن را مطالبه کرده، نباشد. کلاهبرداری های اینترنتی فیشینگ از این ایمیل های جعلی به منظور فریب دادن شما برای افشای نام کاربری و پسورد، سرقت هویت و اطلاعات شما، استفاده می کنند.
2. **کلمه عبور را در کامپیوترهایی که بر روی آن ها کنترل ندارید تایپ نکنید .**کامپیوترهای اشتراکی مانند آن هایی که در کافی نت ها، دانشگاه ها، سالن های کنفرانس و سالن انتظار فرودگاه است، باید در نظر گرفته شود که برای استفاده های شخصی نا امن هستند. از این کامپیوتر ها برای چک کردن آنلاین پست الکترونیک، چت کردن، دیدن صورت حساب های بانکی، و یا هر حساب دیگری که نیاز به یک نام کاربری و رمز عبور دارد، استفاده نکنید. مجرمان از ابزارهای ثبت کردن دکمه های زده شده صفحه کلید استفاده می کنند. این ابزار به افراد خرابکار این امکان را می دهد که تمام اطلاعات تایپ شده بر روی یک کامپیوتر از جمله پسورد شما را از طریق اینترنت به دست آورند.
3. **آن ها را برای دیگران افشا نکنید .**رمز عبور خود را از دوستان و اعضا خانواده (خصوصا کودکان) که می توانند آن را به افراد دیگر منتقل کنند، مخفی نگاه دارید. پسوردهایی که نیاز دارید با دیگران به اشتراک بگذارید، مانند رمز عبور حساب بانکی آنلاین شما که ممکن است با همسر خود به اشتراک گذارید، تنها استثناها هستند.
4. **از پسورد خود محافظت کنید** .مراقب باشید که رمز عبور ذخیره شده و یا یادداشت شده خود را کجا نگه داری می کنید. پسوردها را بر روی یک فایل در کامپیوتر ذخیره نکنید، زیرا که مجرمان ابتدا آن جا را نگاه می کنند. کلمه عبور مورد استفاده خود را در یک مکان امن و مطمئن نگه داری کنید.
5. **رمز عبور خود را به طور منظم تغییر دهید .**با این کار مجرمان و دیگر افراد خرابکار را برای کشف پسورد خود به طور مداوم ناکام می گذارید. هر چه قدرت کلمه عبور شما بیشتر باشد، از آن می توان برای زمان طولانی تر استفاده کرد. پسوردی که کمتر از 8 کاراکتر باشد، باید در نظر گرفته شود که برای حدود یک هفته کارایی دارد، در حالی که پسوردی که 14 کاراکتر یا بیشتر باشد (و از قوانین دیگر ذکر شده در بالا تبعیت کند) می تواند برای چندین سال کارآمد باشد.

با زياد شدن دزد هاي شارژ اينترنت كم كم همه به فكر افتادن تا هر چند روز يك بار رمز واي فاي شان را تغيير بدهند تا ديگر كسي نتواند به شارژ اينترنت شان دسترسي داشته باشد.

شايد مسئله دزدي شارژ اينترنت فقط در ايران مطرح باشد چون در كشورهاي ديگر هزينه شارژ اينترنت انقدر ها زياد نيست كه كسي به فكر دزدي شارژ بيفتد! اما به هر حال تغيير رمز واي فاي در هر جاي دنيا يك مسئله كاملا ضروريست كه در ادامه اين مطلب دليل آن را خدمت شما توضيح ميدهيم.

- **دليل تغيير رمز مودم هاي واي فاي چيست ؟**
- هيچ كسي دوست ندارد كسي بدون اجازه وارد حريم خصوصيش بشود يا اينكه ديگران بدون اجازه از وسايل و لوازم شخصيش استفاده كنند. از اين رو تغيير رمز واي فاي بنا به دو دليل ضروريست:

- **1جلوگيري از دزدي اطلاعات شخصي –**
- متاسفانه خيلي ها اصلا متوجه اين مسئله نيستند كه هكر ها براي دزدي اطلاعات شخصي كاربران چه امكاناتي را در اختيار دارند! سيستم عامل هايي كه عموم مردم از آن استفاده ميكنند امنيت كافي براي محافظت از اطلاعات شخصي شما را ندارند و به راحتي نفوذ پذيرند.
- از طرفي كار كردن با سيستم عامل هاي امن مانند لينوكس براي همه ساده نيست و عموم مردم موقع كار كردن با لينوكس با مشكلات ريز و درشت زيادي مواجه ميشوند. شبكه هاي كامپيوتري بهترين راه براي هكر هاست تا به سيستم شما (چه لپ تاپ چه موبايل) نفوذ كنند و اطلاعات شخصيتان را بدزدند! تغيير مداوم رمز واي فاي دست بسياري از هكر ها رو قطع ميكند. فراموش نكنيد كه تغيير رمز واي فاي فقط يك راه حل ساده است و لازم است بدانيد كه با تغيير رمز واي فاي نميشود هكر هاي حرفه اي رو متوقف كرد!

- **2جلوگيري از دزدي شارژ اينترنت –**
- متاسفانه چون در ايران هزينه اينترنت بسيار بالاست، شارژ دزدي خيلي زياد شده است. اگرچه ريشه اين ناهنجاري فرهنگي صرفا هزينه هاي اينترنت نيست اما مسئله هزينه مي تواند انگيزه شارژ دزدي را در افراد به خصوص نوجوانان ايجاد كند.

# توکن امنیتی

**توکِن امنیتی** یا **نشانهٔ امنیتی** (Security Token) سختافزاری کوچک است که برای ورود کاربر یک سرویس رایانه‌ای به سامانه بهکار میرود. به عبارت دیگر، این دستگاه یک دستگاه فیزیکی است که در اختیار کاربران مجاز قرار میگیرد تا به راحتی بتوانند برای استفاده از یک سیستم کامپیوتری هویت آنها تشخیص داده شود. توکن امنیتی برای اثبات هویت فرد به صورت الکترونیکی استفاده میشود.(به عنوان مثال نحوه دسترسی به حساب بانکی از راه دور). از توکن به علاوه یا به جای رمز عبور معمولی برای احراز هویت مشتری که خواهان ورود به سیستم است، بهره میبرند. به عبارت دیگر به عنوان یک کلید الکترونیکی برای دسترسی عمل میکند.

بعضی از توکنها کلیدهای رمزنگاری مانند امضا دیجیتال و اطلاعات بیومتریک مثل اثرانگشت را در حافظه خود ذخیره میکنند. [1] این توکنها شامل چند کلید برای وارد کردن پینکد یا شماره شناسایی شخصی) و آغاز برنامه توکن برای انجام عملیات ایجاد رمز عبور هستند. طراحی مخصوصی از این توکن به صورت ارتباطUSB و بلوتوث است که این روشها در انتقال کلید رمز تولید شده به سیستم دخالت دارند.

مجموعه‌ای از چند توکن امنیتی با روشهای گوناگون استفاده. در شکل یک سکه یک سنتی برای مقایسه اندازه قرار دارد.

# انواع نشانه و موارد استفاده

- چهار گونه نشانهٔ امنیتی وجود دارد:

1. رمز ثابت
2. رمز پویا با استفاده از الگوریتم متقارن
3. رمز پویا با استفاده از الگوریتم نامتقارن
4. پرسش و پاسخ

- در این نوشته منظور نوع دوم نشانه‌است.
- ساده ترین نوع نشانه نیاز به اتصال به کامپیوتر ندارد. مشتری اعداد را به وسیله صفحه کلیدی که روی صفحه نمایش وجود دارد وارد می‌کند و سپس شماره شناسایی شخصی یا PIN code برای ورود به نشانه را زده وارد می‌شود. هرچند قطع شدن از سرور احراز هویت باعث می‌شود که نشانه‌ها در مقابل حملات میانی آسیب پذیر باشند.
- بعضی از نشانه‌ها به وسیله اتصالات بی سیم به کامپیوتر وصل می‌شوند، مانند بلوتوث .این نوع نشانه‌ها دنباله‌ای از کلید را به مشتری محلی یا نزدیک ترین نقطه دسترسی انتقال می‌دهند.
- نوع دیگر نشانه که امروز خیلی کاربرد وسیعی دارد، تلفن‌های همراه هستند که از ارتباطات در سطح کانال‌های out-of-band مثل صدا، پیام کوتاه، USSDو... استفاده می‌کند. این نوع نشانه نیز همانند نشانه‌های غیر متصل فیزیکی (نوع اول) در مقابل حملات میانی آسیب پذیر هستند.