



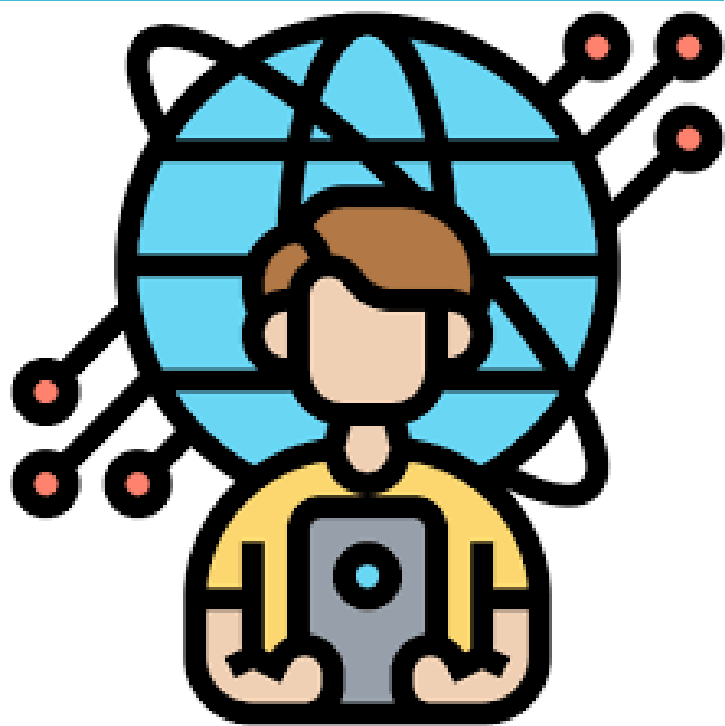
اصول حفظ امنیت در فضای مجازی

دکتر جواد شجاع فرد

عضو هیات علمی دانشگاه علوم توانبخشی و سلامت
اجتماعی



فضای مجازی



فضای مجازی به مجموعه‌ای از محیط‌ها و بسترهای الکترونیکی و اینترنتی گفته می‌شود که در آن افراد، سازمان‌ها و سیستم‌ها می‌توانند بدون حضور فیزیکی و به صورت غیرحضوری با یکدیگر ارتباط برقرار کنند، اطلاعات رد و بدل کنند، محتوا تولید و مصرف کنند یا فعالیت‌های گوناگون (علمی، اقتصادی، اجتماعی، فرهنگی و حتی سیاسی) انجام دهند.

ویژگی‌های اصلی فضای مجازی



غیرمادی بودن: برخلاف فضای واقعی، این فضا لمس پذیر نیست.
جهان ارتباطی: امکان ارتباط سریع و بی‌مرز میان افراد در سراسر جهان.

بی‌زمانی و بی‌مکانی: افراد بدون محدودیت مکانی و زمانی با هم تعامل می‌کنند.

امکان تولید و مصرف محتوا: هر فرد می‌تواند هم مصرف‌کننده و هم تولیدکننده اطلاعات باشد.

تنوع کارکردها: شامل سرگرمی، آموزش، تجارت، سیاست، فرهنگ، پزشکی و غیره.

Percent of individuals who have used the Internet within the past three months



This includes internet use via any mode, such as a computer, mobile phone, personal digital assistant, games machine, digital TV etc.

Source: [International Telecommunication Union via World Bank](#) • [Get the data](#)

مصادیق اصلی فضای مجازی

۱. شبکه‌های اجتماعی

واتساپ، تلگرام، اینستاگرام، توییتر (ایکس)، فیس‌بوک، لینکدین
امکان ارتباط، اشتراک‌گذاری محتوا، شکل‌گیری هویت‌های مجازی

۲. وبسایت‌ها و پورتال‌ها

سایت‌های خبری، فروشگاه‌های، آموزشی و خدماتی
موتورهای جستجو مانند گوگل

۳. بازی‌ها و دنیاهای مجازی

بازی‌های آنلاین چندنفره

محیط‌های واقعیت مجازی (VR) و واقعیت افزوده (AR)

۴. پلتفرم‌های آموزشی و علمی

کلاس‌های آنلاین (شاد، اسکای‌روم، ادوب کانکت، گوگل کلاس روم)
کتابخانه‌های دیجیتال و پایگاه‌های داده علمی



۵. خدمات مالی و اقتصادی دیجیتال

بانکداری اینترنتی و موبایلی

کیف پول‌های الکترونیک و رمزارزها (مثل بیت‌کوین، اتریوم)

تجارت الکترونیک (دیجی کالا، آمازون، علی بابا)

۶. رسانه‌ها و تولید محتوا

یوتیوب، آپارات، اسپاتیفای، پادکست‌ها

بلاگ‌ها و ویکی‌ها (مثل ویکی‌پدیا)

۷. ارتباطات الکترونیکی

ایمیل، پیام‌رسان‌ها، فروم‌ها و گروه‌های گفت‌وگو

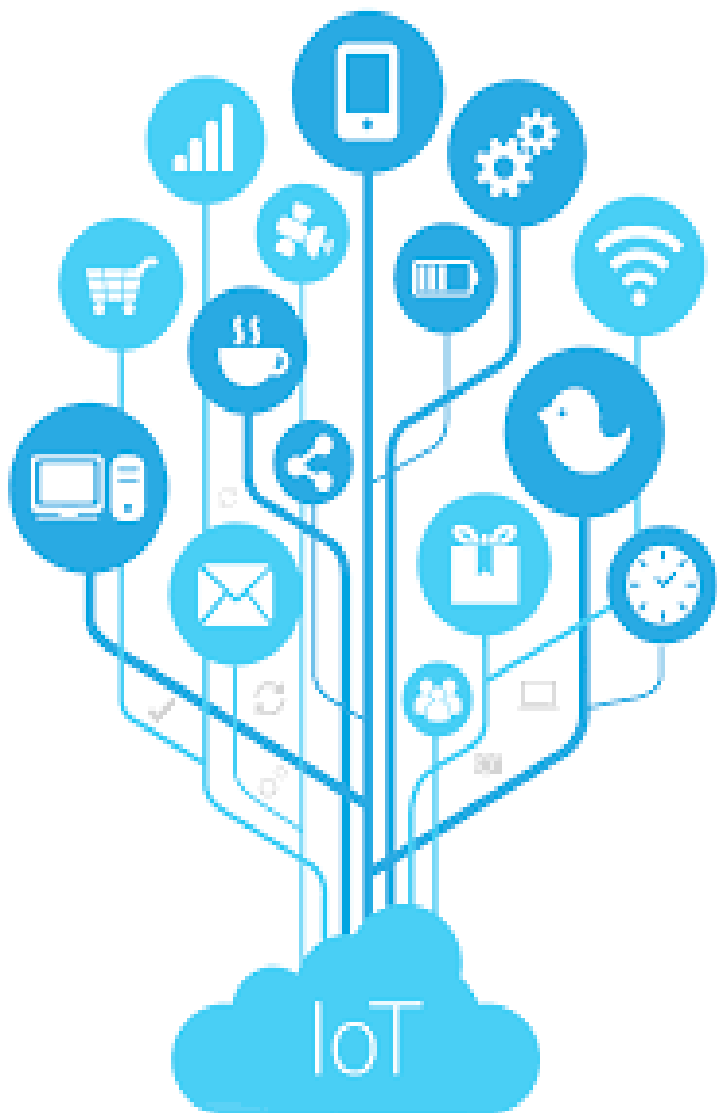
تماس‌های تصویری و کنفرانس‌های آنلاین (Zoom، Google Meet)

۸. زیرساخت‌های فضای مجازی

اینترنت اشیاء (IoT): خانه‌های هوشمند، خودروهای هوشمند

رایانش ابری (Cloud Computing)

شبکه‌های 5G و زیرساخت‌های مخابراتی



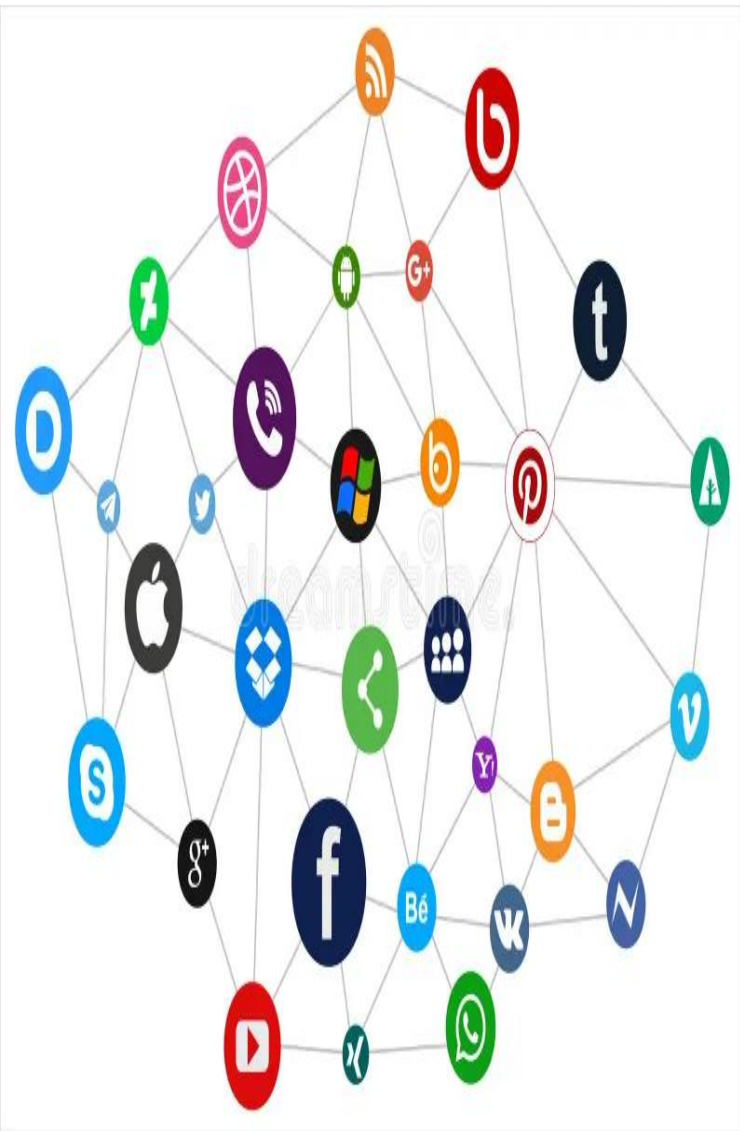
فواید فضای مجازی

۱. جنبه اجتماعی

ارتباط بدون مرز: امکان برقراری ارتباط با دوستان و خانواده در هر نقطه جهان.

تقویت شبکه‌های اجتماعی و حرفه‌ای: ارتباط با همکاران، گروه‌های علمی و انجمن‌های تخصصی.

افزایش مشارکت اجتماعی: افراد می‌توانند در فعالیتهای اجتماعی و کمپین‌های آنلاین شرکت کنند.





۲. جنبه آموزشی و علمی

دسترسی به اطلاعات و منابع آموزشی: کتابخانه‌های دیجیتال، مقالات علمی، دوره‌های آنلاین.

تسهیل یادگیری غیرحضوری: کلاس‌های آنلاین، آموزش از راه دور و ویدئوهای آموزشی.

تقویت مهارت‌های دیجیتال: توانایی کار با نرم‌افزارها، پلتفرم‌ها و ابزارهای دیجیتال



۳. جنبه اقتصادی و حرفه‌ای

تجارت الکترونیک: خرید و فروش آنلاین کالا و خدمات.

کارآفرینی دیجیتال: ایجاد کسب‌وکارهای اینترنتی و کسب درآمد از محتوا یا خدمات آنلاین.

دسترسی به بازارهای جهانی: دسترسی کسب و کارها به مشتریان در سراسر جهان.

۴. جنبه فرهنگی و تفریحی

تبادل فرهنگی: آشنایی با فرهنگ‌ها، زبان‌ها و سبک‌های زندگی مختلف.

سرگرمی و بازی: بازی‌های آنلاین، ویدئوها، موسیقی و فیلم‌های دیجیتال.

ایجاد هویت دیجیتال و بیان خود: می‌توانند اشتراک گذاری افکار و هنر افراد با دیگران.

۵. جنبه علمی-پژوهشی

تحقیق و نوآوری: دسترسی سریع به داده‌ها و تحقیقات علمی.

همکاری علمی بین‌المللی: ارتباط پژوهشگران در پروژه‌های مشترک و ایجاد شبکه‌های همکاری.



چالش ها و مشکلات فضای مجازی

۱. چالش‌های اجتماعی و روانی

اعتیاد به فضای مجازی: استفاده بیش از حد از شبکه‌های اجتماعی، بازی‌ها و اینترنت.

انزوا و کاهش تعاملات واقعی: کاهش ارتباطات حضوری و اجتماعی.

افزایش افسردگی و اضطراب: مقایسه مداوم خود با دیگران در شبکه‌های اجتماعی.

آزار و تهدیدهای آنلاین: قلدری سایبری، تهدید، انتشار شایعات و افترا.



۲. چالش‌های امنیتی و حریم خصوصی

سرقت اطلاعات شخصی: هک، دسترسی غیرمجاز و افشای داده‌ها.
فیشینگ و کلاهبرداری اینترنتی: سرقت رمز عبور، پول یا اطلاعات بانکی.

نظارت و دسترسی غیرمجاز دولت‌ها یا شرکت‌ها: پایش فعالیت‌های کاربران بدون رضایت کامل.



۳. چالش‌های فرهنگی و اخلاقی

انتشار محتوای نامناسب: خشونت، اخبار جعلی، تخریب و نفرت‌پراکنی.
تضعیف ارزش‌ها و هنجارهای اجتماعی: تقلید از رفتارهای نادرست در فضای مجازی.

تحریف واقعیت و شایعه‌پراکنی: انتشار اطلاعات نادرست یا شایعات بدون تأیید.

۴. چالش‌های اقتصادی و شغلی

کلاهبرداری آنلاین و کسب و کارهای ناسالم: تجارت‌های اینترنتی غیرمجاز یا تقلبی.

تأثیر منفی بر بهره‌وری: استفاده غیرهدفمند از فضای مجازی در محیط کار.

عدم شفافیت در بازار دیجیتال: رقابت ناسالم و نبود قوانین دقیق.

۵. چالش‌های آموزشی و علمی

دسترسی محدود به اطلاعات معتبر: غلبه محتوای غیرعلمی و کم کیفیت.

تقلب و کپی‌کاری آنلاین: در امتحانات و پروژه‌های دانشگاهی.

تأثیر منفی بر یادگیری حضوری: کاهش تمرکز و تکیه بر منابع دیجیتال به جای تفکر انتقادی.



انواع تهدیدات امنیت سایبری



فیشینگ

فیشینگ به معنای پنهان کردن کلاهبرداری و ارسال آن به قربانی از طریق پیامک، ایمیل، وبسایت یا تبلیغات آنلاین است. هدف این جرم سرقت اطلاعات، مانند اطلاعات کارت اعتباری و کسب درآمد غیرقانونی است.

بدافزار

این نرم‌افزاری است که توسط مجرم برای دسترسی به رایانه‌ها بدون مجوز طراحی شده است. افراد بدون اطلاع قبلی با دانلود برنامه‌ها از منابع نامعتبر یا مرور وبسایت‌های مشکوک با این برنامه مواجه می‌شوند.

باج افزار

باج افزار نرم افزاری است که برای جلوگیری از دسترسی قربانی به رایانه خود تا زمان پرداخت باج مشخص شده طراحی شده است. با این حال، مجرم می تواند نرم افزار یا داده های رایانه را خراب کند، بنابراین حتی وقتی باج را پرداخت می کنید، تضمینی وجود ندارد که بتوانید آنها را بازیابی کنید.

مهندسی اجتماعی

مهندسی اجتماعی یک تاکتیک فریبنده است که شما را فریب می دهد تا اطلاعات شخصی خود، مانند جزئیات کارت اعتباری را به اشتراک بگذارید. این شکل از تهدید امنیت سایبری می تواند از هر فرم قبلی برای افزایش اعتبار به کلاهبرداری استفاده کند.



امنیت سایبری



امنیت سایبری فرآیند استفاده از پروتکل‌های امنیتی برای محافظت از سیستم‌ها، شبکه‌ها و اطلاعات در فضای مجازی در برابر حملات سایبری است.

مزایای فضای مجازی برای سالمندان

۱. جنبه اجتماعی

- ✓ ارتباط با خانواده و دوستان: تماس تصویری و پیامرسان‌ها باعث کاهش حس تنهایی و انزوا می‌شوند.
- ✓ مشارکت در اجتماعات آنلاین: گروه‌های مجازی ویژه سالمندان، انجمن‌ها و باشگاه‌های اینترنتی.
- ✓ تسهیل فعالیت‌های داوطلبانه: امکان مشارکت در پروژه‌های اجتماعی و کمک به دیگران از راه دور.





۲. جنبه آموزشی

- ✓ دسترسی آسان به منابع آموزشی و دوره‌های آنلاین
- ✓ یادگیری مهارت‌های جدید و به‌روزرسانی اطلاعات
- ✓ استفاده از آموزش‌های مرتبط با سلامت و سبک زندگی
- ✓ استفاده از تجارب دیگران

۳. جنبه سلامت و مراقبت

✓ **دسترسی به اطلاعات سلامت:** مقالات پزشکی، ویدئوهای آموزشی درباره تغذیه، ورزش و بیماری‌ها.

✓ **مشاوره آنلاین پزشکی:** ویزیت و پیگیری درمان بدون نیاز به مراجعه حضوری.

✓ **پیگیری داروها و یادآوری‌ها:** اپلیکیشن‌های یادآور دارو و برنامه‌ریزی سلامت.

✓ **پایش مستمر سلامت:** با استفاده از ابزارهای مبتنی بر اینترنت اشیا



۴. جنبه اقتصادی و خدماتی

✓ خرید و خدمات آنلاین: امکان خرید کالا و خدمات بدون نیاز به رفت و آمد.

✓ دسترسی به بانکداری الکترونیک و پرداخت آنلاین: کاهش مشکلات فیزیکی و رفت و آمد به بانک.

✓ یادگیری مهارت‌های دیجیتال برای کسب درآمد جزئی: کارهای آنلاین ساده یا فروش محصولات خانگی.



۵. جنبه روانی و روحی

- ✓ افزایش اعتماد به نفس: توانایی استفاده از فناوری‌های نوین و مشارکت در زندگی دیجیتال.
- ✓ کاهش اضطراب و افسردگی ناشی از تنهایی: ارتباط مداوم با دیگران و فعالیت‌های سرگرم‌کننده.
- ✓ احساس استقلال و خودکفایی: انجام امور روزمره به صورت دیجیتال بدون وابستگی کامل به دیگران.
- ✓ پر کردن وقت: سرگرمی از طریق بازی‌ها، فیلم‌ها، موسیقی و کتاب‌های دیجیتال.
- ✓ افزایش حس رضایت و نشاط: با مشارکت در فعالیت‌های آنلاین.



سالمندان به عنوان هدفی آسان در حملات سایبری



- ✓ دانش و مهارت و تجربه کم در فضای سایبری
- ✓ مشکلات جسمی مانند کم بینایی
- ✓ اعتماد بیشتر به فضای مجازی
- ✓ حس ترحم و مهربانی و خیر خواهی در سالمندان
- ✓ سوء استفاده از نیازهای عاطفی سالمندان
- ✓ احتمال سارقان در خصوص وضعیت مالی بهتر سالمندان
- ✓ آشنایی کم با تهدیدات سایبری

چرا امنیت سایبری برای سالمندان مهم است؟



امنیت سایبری برای سالمندان مهم است تا حریم خصوصی‌شان حفظ شود و از کلاهبرداری‌ها و تهدیدات سایبری محافظت شوند.



تهدیدات فضای مجازی برای سالمندان

۱. تهدیدات امنیتی و مالی

- ✓ کلاهبرداری آنلاین: فیشینگ، پیام‌های جعلی بانکی، خریدهای تقلبی.
- ✓ سرقت اطلاعات شخصی: سوءاستفاده از اطلاعات هویتی یا رمزهای عبور.
- ✓ تقلب در سرمایه‌گذاری دیجیتال: وعده‌های دروغین کسب درآمد یا رمزارزها.

۲. تهدیدات اجتماعی و روانی

- ✓ تنهایی دیجیتال: جایگزینی کامل ارتباط حضوری با ارتباط مجازی که ممکن است اثرات منفی روانی داشته باشد.
- ✓ احساس اضطراب و سردرگمی: در مواجهه با فناوری‌های جدید یا تغییرات سریع در پلتفرم‌ها.
- ✓ آزار و تهدید آنلاین: پیام‌های تهدیدآمیز یا توهین‌آمیز، حتی در شبکه‌های اجتماعی.





۳. تهدیدات فرهنگی و اطلاعاتی

- ✓ انتشار اطلاعات نادرست و شایعات: سالمندان ممکن است اخبار جعلی را باور کنند یا منتشر کنند.
- ✓ محصولات یا محتوای نامناسب: تبلیغات، بازی‌ها و ویدئوهای ناسازگار با سن و فرهنگ سالمندان.
- ✓ فشار اجتماعی و تبلیغات هدفمند: تشویق به خرید غیرضروری یا تغییر سبک زندگی بدون آگاهی کامل.
- ✓ افشاء اطلاعات شخصی: سالمندان ممکن است به دلایل مختلف، اطلاعات شخصی خود را فاش کنند.

۴. تهدیدات سلامتی

✓ افزایش آسیب‌های فیزیکی و بینایی: استفاده طولانی مدت از صفحه‌نمایش باعث خستگی چشم، کم‌تحرکی و مشکلات جسمی می‌شود.

✓ اختلالات خواب و ذهنی: استفاده بیش از حد شبانه از شبکه‌های اجتماعی یا بازی‌ها.

✓ افزایش استرس و اضطراب ناشی از فناوری: فشار روانی برای یادگیری ابزارهای جدید یا مواجهه با مشکلات فنی

✓ انجام اقدامات آسیب‌رسان به سلامت: در اثر مشاهده اطلاعات نادرست و جعلی.

✓ استفاده از کالاهای فاقد اصالت یا فاقد اثر یا زیان‌رسان به سلامت: در اثر پیروی از تبلیغات غیر واقعی.



راهکارهای افزایش امنیت سالمندان در فضای مجازی



۱. آموزش و آگاهی بخشی

✓ آموزش پایه دیجیتال: نحوه استفاده از اینترنت، پیام‌رسان‌ها و شبکه‌های اجتماعی.

✓ آشنایی با تهدیدات رایج: فیشینگ، پیامک‌ها و ایمیل‌های مشکوک، تبلیغات دروغین.

✓ تمرین تشخیص سایت‌ها و اپلیکیشن‌های امن: توجه به آدرس وبسایت و نمادهای امنیتی (مثل HTTPS).

✓ شناسایی فعالیت‌های مشکوک در فضای مجازی: درخواست اطلاعات حساس مانند رمز دوم کارت بانکی



۲. مدیریت حساب‌ها و رمز عبور

✓ استفاده از رمز عبور قوی و متفاوت برای هر حساب کاربری.

✓ فعال‌سازی احراز هویت دو مرحله‌ای برای ایمیل و شبکه‌های اجتماعی.

✓ به‌روزرسانی منظم رمزها و عدم اشتراک‌گذاری آن‌ها با افراد ناشناس

۳. کنترل دسترسی و حریم خصوصی

✓ تنظیم حریم خصوصی در شبکه‌های اجتماعی: محدود کردن دسترسی افراد غریبه به اطلاعات شخصی.

✓ محدود کردن دسترسی اپلیکیشن‌ها به داده‌ها: GPS، دوربین، میکروفن و اطلاعات شخصی.

✓ آگاهی از خطرات اشتراک‌گذاری بیش از حد اطلاعات: حتی با دوستان آنلاین.





۴. استفاده از ابزارهای امنیتی

- ✓ نصب نرم افزارهای آنتی ویروس و فایروال برای محافظت از دستگاه‌ها.
- ✓ به روز رسانی سیستم عامل و اپلیکیشن‌ها به صورت منظم.
- ✓ مسدود سازی ایمیل‌ها و پیام‌های مشکوک و عدم کلیک روی لینک‌های ناشناس.



۵. مدیریت خرید و تراکنش‌های آنلاین

- ✓ استفاده از روش‌های پرداخت امن: کارت‌های بانکی با رمز دوم و اپلیکیشن‌های معتبر.
- ✓ بررسی دقیق فروشگاه‌ها و سایت‌های خرید آنلاین قبل از وارد کردن اطلاعات مالی.
- ✓ عدم اعتماد به پیشنهادهای مالی و سرمایه‌گذاری آنلاین بدون تحقیق کامل.

۶. حمایت خانواده و مراقبان

✓ همراهی در مراحل استفاده از اینترنت و آموزش مرحله به مرحله.

✓ نظارت غیرتهاجمی بر فعالیت آنلاین سالمندان بدون محدود کردن استقلال آنها.

✓ تشویق به تعامل اجتماعی حضوری همراه با حضور آنلاین تا توازن حفظ شود.

۷. مراقبت از اطلاعات شخصی و مهم

✓ جلوگیری از دسترسی افراد غیر مجاز

✓ تهیه نسخه پشتیبان از اطلاعات و نگهداری در مکان امن

✓ عدم انتشار اطلاعات غیر ضروری و حساس در فضای مجازی

✓ رمز گذاری اطلاعات و دستگاههای حاوی اطلاعات

✓ دانلود ایمن برنامه‌ها از سایتهای معتبر مانند بازار، گوگل پلی،
اپ استور و ...

✓ محافظت از اطلاعات مالی (در زمان استفاده از خودپردازها)

✓ عدم اجازه دسترسی افراد غیر مجاز به رایانه و تلفن همراه



ایجاد رمزهای عبور قوی

✓ در انتخاب رمز، از استفاده از اطلاعات شخصی خودداری کنید (نام اعضای خانواده، تاریخ‌های مهم مانند تولد یا سالگرد ازدواج، کد ملی، شماره تلفن و ...)

✓ عباراتی را انتخاب کنید که با اعداد و نمادهایی ترکیب شده‌اند که هیچ ارتباط آشکاری با زندگی شخصی شما ندارند.

✓ از یک رمز عبور طولانی‌تر استفاده کنید (حداقل ۱۲-۱۵ کاراکتر)

✓ از ترکیبی از نمادها، اعداد و حروف بزرگ و کوچک استفاده کنید.
(P@3\$WorDJ@dID#)

✓ از کلمات یا عبارات رایج اجتناب کنید (نام شهر، محله، خیابان)

✓ از نرم افزارهای مدیریت رمز استفاده کنید.



ایجاد رمزهای عبور قوی (ادامه)

- ✓ از احراز هویت دو عاملی استفاده کنید (پیامک یا ایمیل و پسورد)
- ✓ رمزهای عبور را برای سایت‌های مختلف سفارشی کنید (عدم استفاده از یک رمز عبور برای همه حسابها)
- ✓ از نوشتن رمزهای عبور خودداری کنید.
- ✓ ایمیل بازیابی و شماره تلفن اضافه کنید.
- ✓ به روزرسانی منظم رمزهای عبور.



شناسایی موارد مشکوک

ایمیل‌های کلاهبرداری می‌توانند واقعی به نظر برسند و وانمود کنند که از مکان‌های رسمی مانند بانک ارسال شده‌اند، اما باید مراقب موارد زیر باشید:



- ✓ اشتباهات املایی یا دستوری، یا سبک نگارش غیرمعمول
- ✓ آدرس‌ها یا فرستندگان ایمیل غیررسمی یا مشکوک
- ✓ درخواست اطلاعات شخصی، مانند نام کاربری، رمز عبور کامل یا اطلاعات بانکی شما - سازمان‌های واقعی هرگز این را نمی‌خواهند.
- ✓ تهدید می‌کنند که اگر همین الان اقدام نکنید، معامله منقضی می‌شود یا حساب شما بسته می‌شود یا حقوق بازنشستگی و بیمه شما قطع می‌شود.
- ✓ درخواست می‌کنند روی لینک خاصی کلیک کنید.

سپاس از توجه شما

