فصل ۶

کار با شبکه‌های اجتماعی

هدف کلی

توانایی کار با شبکه‌های اجتماعی

هدف‌های رفتاری

پس از مطالعه این فصل از هنرجو انتظار می‌رود که:

- با مفاهیم کاربردی در شبکه‌های اجتماعی آشنا شود.
- با انواع نرم‌افزارهای شبکه اجتماعی کاربردی آشنا شود.
- با جرائم رایانه‌ای آشنا شود.
- با اخلاقیات آنلاین، حفظ حریم خصوصی افراد و رعایت حقوق شهروندی آشنا شود.
- نصب برنامه‌های مورد نیاز و تنظیمات و فعال‌سازی شبکه‌های اجتماعی را انجام دهد.

زمان (ساعت)	
نظری	عملی
۲	۳

مقدمه

امروزه دنیای مجازی، به ملموس‌ترین واقعیت زندگی اجتماعی ما تبدیل شده، سبک زندگی بسیاری از ما را دستخوش تغییرات کرده و حجم زیادی از اصطلاحات جدید را به فرهنگ لغت روزانه ما، وارد نموده است. در این فصل با مفهوم «Social Network» یا شبکه‌های اجتماعی که در قالب اپلیکیشن در تلفن‌های همراه هوشمند و رایانه و لپ‌تاپ از آنها استفاده می‌کنیم، بررسی خواهیم کرد.

لازم است بدانیم استفاده از هرگونه شبکه اجتماعی نیاز به داشتن مهارت‌های اجتماعی، سوادرسانه‌ای، زبان‌های خارجی و فناوری اطلاعات دارد.

شبکه‌های اجتماعی Social Network

شبکهٔ اجتماعی، ساختاری اجتماعی است که از گروه‌هایی (عموماً فردی یا سازمانی) تشکیل شده‌است که توسط یک یا چند نوع خاص از وابستگی مانند ایده‌ها و تبادلات مالی، دوستان، خویشاوندان، لینک‌های وب، به هم وصل هستند. اصطلاح **شبکه‌های اجتماعی** یک مفهوم عمومی و بسیار گسترده است که به همهٔ انواع شبکه‌های اجتماعی انسانی و گروه‌های اجتماعی انسان‌ها اشاره دارد و آن را نمی‌توان در چند ابزار مانند اینستاگرام، توئیتر و یوتیوب خلاصه کرد. شبکه‌های اجتماعی به یک پلتفرم نیاز دارند.

نمونه‌های رایج سایت‌ها یا پلتفرم‌های شبکه‌های اجتماعی شامل فیس‌بوک، اینستاگرام، توئیتر و لینکدین است. کاربران به یک پلتفرم شبکه اجتماعی می‌پیوندند و شروع به برقراری ارتباط (یا شبکه) با سایر کاربران می‌کنند. این کار به این دلیل انجام می‌شود که کاربران بتوانند انتخاب کنند که از چه کسی می‌خواهند ارتباطات را دریافت کنند. در برخی موارد، ارتباط یک‌طرفه است، در حالی که در برخی دیگر، دو طرفه یا چند جهته است.

شکل ۱ـ۶ـ مدل مفهومی شبکه‌های اجتماعی

رسانه‌های اجتماعی Social Media

رسانه اجتماعی از دو واژه «رسانه» به معنای بستر یا وسیله ارسال پیام و «اجتماعی» که در اینجا منظور دریافت گروهی همان پیام است، تشکیل شده است رسانه اجتماعی مجازی عبارت است از بسترهای مبتنی بر فناوری که زمینه ارتباط، تعامل و گردهمایی برای تولید و مصرف محتوا را فراهم می‌کنند. یکی از مهم‌ترین ویژگی‌های رسانه‌های اجتماعی مجازی شکل‌گیری فضای ارتباطی است که در آن مشارکت‌کنندگان یا حاضران که کاربران هم نامیده می‌شوند، هم‌زمان هم تولید کننده اطلاعات هستند و هم مصرف‌کننده آن.

شکل ۲ـ۶ـ مدل مفهومی رسانه‌های اجتماعی

رسانه‌های اجتماعی به مجموعه سایت‌ها و ابزارهایی اطلاق می‌شود که در فضای ایجاد شده به‌وسیله رسانه‌های نوین از قبیل شبکه‌های ارتباطی، اینترنت و تلفن‌های همراه، متولد شده‌اند و رشد پیدا کرده‌اند. باید بدانیم این رسانه‌های اجتماعی نوین، ویژگی‌های ارتباطی متفاوتی با رسانه‌های سنتی دارند. از این‌رو گاهی در مقابل رسانه‌های قدیمی‌تر از جمله تلویزیون، رادیو، کتاب و مطبوعات، برای رسانه‌های دنیای مجازی از عبارت رسانه‌های اجتماعی استفاده می‌شود. اساساً رسانه‌های اجتماعی بستری برای پخش اطلاعات هستند، هر کسی می‌تواند رسانه‌های اجتماعی را منتشر کند. رسانه‌های خبری سنتی، مانند CNN و فاکس نیوز، محتوای خود را برای مصرف دیجیتال منتشر می‌کنند. کسب و کارها و سازمان‌ها نیز این کار را انجام می‌دهند.

تفاوت شبکه‌های اجتماعی و رسانه‌های اجتماعی: در حالی که به نظر می‌رسد اصطلاحات رسانه‌های اجتماعی و شبکه‌های اجتماعی قابل تعویض هستند، تفاوت‌های مشخصی دارند. اساساً رسانه‌های اجتماعی بستری برای پخش اطلاعات هستند، در حالی که شبکه‌های اجتماعی بستری برای برقراری ارتباط با یکدیگر هستند. رسانه‌های اجتماعی یک کانال ارتباطی هستند، در حالی که در شبکه‌های اجتماعی، ارتباط، ماهیتی دو طرفه دارد.

آشنایی با تاریخچه شبکه‌های اجتماعی اینترنتی

نخستین بار مفهومی با عنوان شبکه‌های اجتماعی اینترنتی با قالب امروزی درسال ۱۹۶۰ اولین‌بار در دانشگاه ایلی نویز در ایالت متحده آمریکا مطرح شد. پس از آن درسال ۱۹۹۷ نخستین سایت شبکه

شکل ۳ـ۶

اجتماعی اینترنتی به آدرس Sixdegrees.com راه‌اندازی شد. این سایت به کاربرانش اجازه ایجاد پروفایل داد تا آنها بتوانند لیستی از دوستانشان ایجاد کنند. البته این سایت در آن موفق نشد و بعد از سه سال متوقف شد.

بعد از آن، انفجار تجارت در وب سایت‌های اجتماعی در سال ۲۰۰۲ باعث به‌وجود آمدن شبکه‌های اجتماعی فرنداستر (Friendster)، اورکات (Orkut) و لینکداین (Linkedin) شد و باعث شکوفایی قارچ‌گونه وب سایت‌های شبکه‌های اجتماعی در اینترنت شد.

در سال ۲۰۰۴، سایت‌های شبکه اجتماعی فرنداستر با ۷ میلیون کاربر و مای اسپیس با ۲ میلیون کاربر صاحب بیشترین کاربران در این حوزه بودند. در همین سال سایت شبکه اجتماعی فیسبوک توسط مارک زوکربرگ در خوابگاه دانشگاه‌هاروارد راه اندازی شد.

سال ۲۰۰۶، سال گسترش روزافزون کاربران و بازدیدکنندگان وب‌سایت‌های شبکه‌های اجتماعی بود. در این سال دسترسی عمومی مردم به فیسبوک آزاد شد، زیرا در دو سال قبل، این سایت تنها به‌صورت پایلوت در دانشگاه‌هاروارد استفاده می‌شد، همچنین توییتر نیز در این سال پا به عرصه وب سایت‌های اجتماعی گذاشت.

اهداف شبکه‌های اجتماعی

اهداف بسیار زیادی را می‌توان برای شبکه اجتماعی مجازی نام برد که برخی از مهم‌ترین آنها به‌ترتیب زیر است:

- فراهم کردن بستری برای اینکه افراد بتوانند نظرات خودشان را با دیگران به اشتراک بگذارند.
- ایجاد یک پایگاه داده از کاربران و خصوصیات آنها که می‌توان از آنها برای آنالیز جامعه و برنامه‌ریزی‌های بعدی استفاده نمود.
- ایجاد رفاه و امکانات بیشتر برای سرعت بخشیدن به انتقال اطلاعات.
- به‌وجود آمدن نوعی عدالت و برابری که هر فرد بتواند ایده‌های خودش را مطرح نماید.
- آشنا نمودن جوامع مختلف با آیین و رسوم یکدیگر. به‌نظر می‌رسد که شبکه اجتماعی مجازی گامی دیگر در جهت تبدیل شدن دنیا به یک جزیره کوچک و کوچک‌تر بوده است.

به‌طورکلی، شبکه‌های اجتماعی دارای مزایای متنوعی هستند که مورد پسند بسیاری از افراد جامعه قرار گرفته‌اند. با این حال، گاهی اوقات صحبت‌هایی در مورد برخی از شبکه‌های اجتماعی می‌شود که زیاد خوشایند نیست. به‌عنوان مثال، بعضی مواقع هدف دسترسی به اطلاعات شخصی کاربران را جزء ویژگی‌های شبکه‌های اجتماعی می‌دانند.

انواع شبکه‌های اجتماعی

نوع هر شبکه اجتماعی مجازی را می‌توان از لحاظ فاکتورهای مختلفی بررسی نمود.

- شبکه‌های اجتماعی تصویر محور: به‌عنوان مثال از لحاظ محتوا، شبکه اینستاگرام تصویر محور است.
- شبکه‌های اجتماعی ویدیو محور: مانند تیک‌تاک
- شبکه‌های اجتماعی گفت‌وگو محور: مانند Reddit و Quora
- شبکه‌های اجتماعی وبلاگی و انجمن

شبکه‌های اجتماعی خارجی

شبکه اجتماعی فیسبوک Facebook: شبکه اجتماعی محبوبی می‌باشد که به کاربران اجازه اشتراک‌گذاری فیلم، عکس و ایجاد چت به‌صورت صوتی، تصویری و نوشتاری را می‌دهد. فیسبوک از محبوب‌ترین‌های شبکه‌های اجتماعی در حال حاضر می‌باشد.

شبکه اجتماعی یوتیوب Youtube: یوتیوب، بزرگ‌ترین و محبوب‌ترین رسانهٔ تصویری در بین شبکه‌های اجتماعی مجازی است که در ۱۴ فوریه سال ۲۰۰۵ با همکاری سه کارمند سابق پی پال، تأسیس و بعدها در نوامبر ۲۰۰۶ به قیمت ۱.۶۵ میلیارد دلار توسط کمپانی گوگل، خریداری شد. این وب‌سایت در حال حاضر، بیش از ۱ میلیارد و ۵۰۰ میلیون بازدید ماهانه دارد اما از شبکه‌های اجتماعی نمونه یوتیوب در شبکه اجتماعی ایرانی می‌توان آپارات را نام برد.

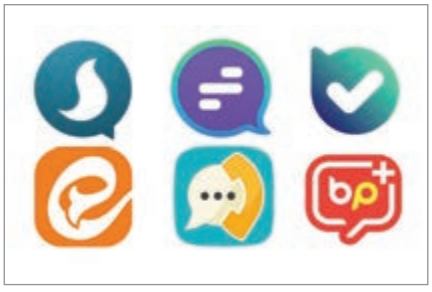
شبکه اجتماعی اینستاگرام Instagram: اینستاگرام یک شبکه اجتماعی تصویری است. این پلتفرم در ۶ اکتبر سال ۲۰۱۰ راه‌اندازی شد و بیش از ۴۰۰ میلیون کاربر فعال دارد و مالک اصلی اینستاگرام هم، فیسبوک است. تعداد بسیار زیادی از کاربران از این شبکه برای پست‌کردن تصاویر سفر خود، دنیای مد، غذاهای مختلف و مورد علاقه خود، هنر و سایر موضوعات مشابه استفاده می‌کنند. در این فضا شما می‌توانید به‌راحتی و تنها با چند ترفند افزایش فالوور در اینستاگرام خود داشته باشید.
یکی از دلایل محبوبیت اینستاگرام، به واسطهٔ فیلترهای منحصر به فردی است که امکانات ویرایش عکس و ویدیو را، ایجاد می‌کنند. تقریباً ۹۵ درصد کاربران این شبکه عضو فیسبوک هم هستند و بدین‌ترتیب شما می‌توانید با یک تیر دو نشان را هدف بگیرید. هم‌اکنون اینستاگرام حدود ۸۰۰ میلیون بازدید ماهانه دارد.

شبکه اجتماعی توئیتر Twitter: توییتر در ۲۱ مارس سال ۲۰۰۶ تأسیس شد و دفتر اصلی آن در سان‌فرانسیسکوی کالیفرنیا است. شاید این پرسش به ذهن شما هم رسیده باشد که ارسال پست با استفاده از حداکثر ۲۸۰ کاراکتر درتوییتر، روش مناسبی برای تبلیغات تجاری نیست اما بنابر آمار، این رسانهٔ ارتباط اجتماعی بیش از ۳۲۰ میلیون کاربر ماهانهٔ فعال دارد که با استفاده از همین محدودیت ۲۸۰ کاراکتری اطلاعات خود را انتقال می‌دهند. در زمینه تجارت، مشاغل مختلف از این رسانهٔ پربیننده برای تعامل با مشتریان خود، پاسخ‌دهی به سؤالات آنها و انتشار آخرین اخبار استفاده می‌کنند و هم‌زمان تبلیغات ویژه برای مخاطبین خاص خود را هم، پیگیری می‌کنند.

شبکه‌های اجتماعی ایرانی

شبکه اجتماعی بله Bale: این شبکه اجتماعی مجازی، در سال ۱۳۹۵ شمسی راه‌اندازی شد. به‌وسیله شبکه بله می‌توان علاوه بر ارسال پیام، به انجام امورات مالی نیز پرداخت. یکی از اصلی‌ترین پشتوانه‌های این شبکه اجتماعی بانک ملی ایران می‌باشد.

شبکه اجتماعی ایتا: یک سال پس از بله و در سال ۱۳۹۶ شروع به‌کار نمود. نمایش محتوای آن شبیه به اینستاگرام بوده و همین‌طور امکان انتقال وجه را فراهم کرده است.



شکل ۴ـ۶ـ آیکن‌های شبکه‌های اجتماعی ایرانی

شبکه اجتماعی روبیکا: این شبکه اجتماعی مجازی همه‌کاره می‌باشد و از طرفی پرحاشیه هم بوده است. در سال ۱۴۰۰ مجوز اپلیکیشن روبیکا به‌دلیل ساخت حساب برای کاربران بدون مجوز، باطل شد.
شبکه اجتماعی آی‌گپ: این پیام‌رسان از امنیت بالا و کیفیت مطلوبی جهت نگهداری و تبادل داده‌ها برخوردار می‌باشد. در سیستم عامل‌های اندروید، iOS، لینوکس، ویندوز و تحت وب اجرا می‌گردد.
شبکه اجتماعی سروش: در ابتدا، کار خودش را با حمایت صدا و سیما آغاز نمود و هم اکنون به‌صورت مستقل فعالیت می‌کند. همچنین نام او به سروش پلاس تغییر یافت.
شبکه اجتماعی شاد: نام این شبکه اجتماعی مجازی، مخفف عبارت شبکه آموزشی دانش‌آموز است. یکی از علت‌های پیدایش شاد، فراگیر شدن ویروس کرونا بود. این پیام‌رسان در دوران شیوع کرونا، نقش مهمی در برگزاری آنلاین کلاس‌های درس داشته است.

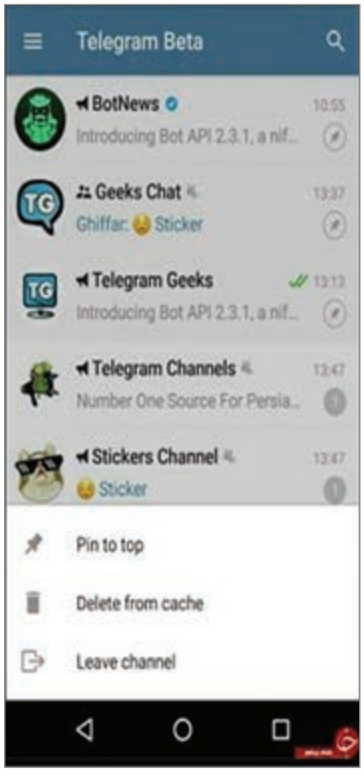
تحقیق

در مورد تفاوت شبکه اجتماعی روبیکا و سروش مطلب جمع‌آوری نمایید و راجع به مزایا و معایب و کاربرد هریک در کلاس بحث و گفت‌وگو نمایید.

۱ـ۶ـ مفاهیم کاربردی در شبکه‌های اجتماعی

۱ـ۱ـ۶ـ Like ,Post ,Direct , Forward و Pin

Post: کل مطالب منتشر شده توسط صاحب پیج (اعم از عکس، فیلم و متن) را پست می‌گویند.
Like: به معنی علاقه داشتن است. شما می‌توانید برای پست‌هایی که در اینستاگرام مشاهده می‌کنید، از لایک استفاده کنید. لایک یعنی رضایت شما از محتوای پست موردنظر. درنظر داشته باشید اگر پستی را لایک کنید و بعداً پشیمان شوید به‌راحتی می‌توانید لایک آن پست را پاک کنید.
Direct: به معنی مستقیم و بدون واسطه می‌باشد. در اینستاگرام به ارسال پیام خصوصی برای فرد مورد نظرتان دایرکت می‌گویند.
Forward: فوروارد در شبکه‌های اجتماعی به معنی فرستادن پیغام یا پست یک شخص به یک شخص دیگر می‌باشد. این امکان توسط خود شبکه اجتماعی مربوطه فراهم می‌شود و به واسطه آن می‌توانید پیامی را برای دوستان خود انتقال دهید.
Pin: شما می‌توانید گروه، کانال و یا چت‌های خاص و مهم را به بخش بالایی صفحه و یا لیست چت‌ها را **pin** کنید تا همواره در دسترس و دید عموم قرار بگیرد.



شکل ۵ـ۶ـ صفحه تلگرام

پین‌کردن کانال یا گروه به اول صفحه: ابتدا برنامه خود (شاد، تلگرام و..) را به‌روزرسانی کرده و آن را اجرا کنید. سپس انگشت خود را روی کانال یا گروه موردنظر نگه‌داشته و سپس گزینه Pin to top را انتخاب کنید.
در برنامه شاد نیز به همین ترتیب می‌باشد با این تفاوت که کلمه «سنجاق کردن به بالا» را باید انتخاب نمایید.
درصورتی‌که قصد دارید این گروه یا کانال را از بالای صفحه حذف کنید، مجدداً باید انگشت خود را روی نام آن نگه‌داشته و گزینه Unpin to top را انتخاب کنید.
پین‌کردن پیام در گروه‌ها و کانال‌ها: برای پین کردن پیام در گروه‌ها و کانال‌ها، انگشت خود را روی کانال یا گروه موردنظر نگه‌داشته و سپس گزینه «سنجاق پیام» را انتخاب کنید.
درصورتی‌که قصد دارید این پیام را از بالای صفحه حذف کنید، مجدداً باید انگشت خود را روی نام آن نگه‌داشته و گزینه «برداشتن سنجاق» را انتخاب کنید.

۲ـ۶ـ معرفی چند نرم‌افزار شبکهٔ اجتماعی کاربردی

۱ **فیسبوک:** بزرگ‌ترین شبکه اجتماعی دنیا با بیش از ۲ میلیارد کاربر فعال در ماه است. فیسبوک محلی مناسب برای تعامل با دوستان و آشنایان، بیزینس و تجارت و همچنین تبلیغات است. اشتراک‌گذاری مطالبتان در پیج تجاری فیسبوک بسیار روی سئو تأثیرگذار است.
۲ **واتساپ:** واتساپ یک شبکه اجتماعی مبتنی بر پیام است که الان جزئی از فیسبوک می‌باشد و در سال ۲۰۱۷ بیش از ۱ میلیارد نفر کاربر فعال داشته است.
۳ **لینکدین:** یک شبکه اجتماعی مرتبط با مشاغل و صاحبان کسب و کار است که متعلق به ماکروسافت بوده و تاکنون بیش از ۵۰۰ میلیون عضو دارد. فعال بودن حساب اعضای یک کسب و کار در لینکدین بسیار بر روی سئو و بازخورد یک کسب و کار تأثیرگذار است.
۴ **توییتر:** توییتر دارای بیش از ۱۴۰ میلیون کاربر است که بیشتر در کشور آمریکا محبوب بوده و کاربران می‌توانند تا ۱۴۰ کاراکتر را برای هم به همراه عکس و ویدیو توییت کنند.
۵ **اینستاگرام :** شبکه اجتماعی متکی بر عکس و ویدیو که متعلق به فیسبوک بوده و بیش از ۳۷۵ میلیون عضو دارد و در کشور ما، ایران نیز بسیار محبوب است.
۶ **پینترست:** یک شبکه اجتماعی مبتنی بر اشتراک‌گذاری تصویر و ویدیو از سایت‌های دیگر است که به قول خود سایت، آنها را پین می‌کند و در آلبوم‌هایی که شما تعیین می‌کنید نمایش می‌دهد.

تحقیق

چند مورد از شبکه‌های خارجی، غیر از موارد بالا را جست‌وجو کرده و در کلاس درباره آنها بحث نمایید.

۷ **شبکه اجتماعی دانشجویی روبرد:** یکی از شبکه‌های اجتماعی ایرانی است که امکان استفاده از آن برای چهار زبان فارسی، انگلیسی، ترکی استانبولی و عربی وجود دارد. این پیام‌رسان در چهارچوب فرهنگ ایرانی ساخته شده است.
۸ **شبکه اجتماعی پیام‌رسان سروش و سروش پلاس:** اپلیکیشن سروش جزء بهترین شبکه اجتماعی ایرانی محسوب می‌شود. پیام‌رسان سروش نسخه ایرانی تلگرام است که کاربران زیادی را به خود جذب کرده است. در سال‌های اخیر و با تعطیلی مدارس به‌دلیل کرونا، این شبکه اجتماعی برای تحصیل مجازی مورد

استفاده قرار گرفت. سروش پلاس آخرین و بهترین آپدیت این اپلیکیشن است. سروش پلاس از فرمت بهتری برخوردار است و حاوی یک دستیار صوتی است که می‌توان تنظیمات، پیام‌ها، تماس‌ها و... را به آسانی انجام داد. همچنین سروش پلاس قسمتی به نام Post Chin یا Time Line دارد که حاوی بهترین پست‌های کانال است. در این نسخه علاوه بر دستیار صوتی و Time Line، امکانات دیگری مانند تماس صوتی و تصویری، VOD و تلویزیون، پخش زنده (Live) نیز وجود دارد. البته باید گفت که برخی از این قابلیت‌ها در نسخه iOS سروش پلاس وجود ندارند.

۹ **شبکه اجتماعی پیام‌رسان نزدیکا:** پیام‌رسان نزدیکا یک شبکه اجتماعی ایرانی است که شبیه به اینستاگرام است و می‌توان آن را اینستاگرام ایرانی در نظر گرفت. کاربران می‌توانند به کمک این شبکه اجتماعی با دوستان خود در ارتباط باشند و با کاربران جدیدی آشنا شوند.

۱۰ **شبکه اجتماعی پیام‌رسان روبیکا:** پیام‌رسان روبیکا یکی از بهترین اپلیکیشن‌ها است که تمامی قابلیت‌های شبکه‌های اجتماعی را دارد و درواقع ترکیبی از همه آنها است. همچنین روبیکا انواع فیلم و سریال‌های جدید را ارائه می‌دهد که به همین دلیل کاربران زیادی را به خود جذب کرده است.

۱۱ **شبکه اجتماعی پیام‌رسان آی‌گپ:** آی‌گپ یک شبکه اجتماعی ایرانی برای تبادل عکس، ویدیو، پیام متنی و... است. همچنین با تغییر سایت‌های دانشگاه‌ها، این اپلیکیشن مورد استفاده دانشجویان قرار گرفته است.

۱۲ **شبکه اجتماعی پیام‌رسان طاقچه:** پیام‌رسان طاقچه مربوط به نویسندگی و کتاب‌خوانی است که کاربران می‌توانند با استفاده از آن کتابی را منتشر یا دانلود کنند. این پلتفرم جهت حمایت از نویسندگان و گسترش فرهنگ کتاب و کتاب‌خوانی ساخته شده است.

۱۳ **شبکه اجتماعی پیام‌رسان ایتا:** پیام‌رسان ایتا شبیه به تلگرام است و امکان ایجاد کانال و گفت‌وگو در آن وجود دارد. این پلتفرم با هدف جایگزینی تلگرام به بازار عرضه شده است.

تحقیق

چند مورد از شبکه‌های ایرانی، غیر از موارد بالا را جست‌وجو کرده و در کلاس راجع به آنها بحث نمایید.

۱ـ۲ـ۶ـ برنامه‌های مورد نیاز جهت نصب شبکه‌های اجتماعی

برای نصب شبکه‌های اجتماعی، از گوگل‌پلی در گوشی‌های اندرویدی و از اپ‌استور در گوشی‌های اپل استفاده می‌شود.

از برنامه‌های دیگری که می‌توان استفاده کرد برنامه مایکت و برنامه بازار را می‌توان نام برد.

۲ـ۲ـ۶ـ فعال‌سازی و تنظیمات اولیه شبکه‌های اجتماعی

پس از دانلود نرم‌افزارهای شبکه‌های اجتماعی شروع به نصب آن می‌کنیم.

در طی مراحل نصب اپلیکیشن از شما کد فعال‌سازی درخواست می‌شود که پس از دریافت آن، آن را وارد نمایید.

بعد از راه‌اندازی اپلیکیشن شبکه اجتماعی موردنظر نیاز به تنظیمات آن خواهید داشت.

تنظیمات و مدیریت گروه‌ها در بله: گروه‌ها و کانال‌های بله، یکی از امکانات کاربردی بله است که به وسیلهٔ آن می‌توانید ارتباطات کاری و شخصی‌تان را گسترش دهید. گروه‌های بله امکانات زیادی را در اختیار ما قرار می‌دهند و تنظیماتی دارند که ممکن است از آنها آگاه نباشیم.

ساخت گروه در بله: در بله به‌راحتی می‌توانید گروه بسازید و تنظیمات مختلف روی گروه انجام دهید. در

این قسمت تنظیمات مختلف گروه را به شما معرفی می‌کنیم و آموزش می‌دهیم که چگونه در بله گروه را ببندیم و گروه‌های بله را خصوصی کنیم. برای ساخت گروه در بله این مراحل را طی کنید:

۱ در صفحهٔ اصلی اپلیکیشن بله، زبانهٔ مخاطبین را انتخاب کنید. اگر از نسخهٔ اندروید استفاده می‌کنید، علاوه بر روش قبل، می‌توانید در زبانهٔ گفت‌وگو، منوی مخاطبین (منوی گرد سبز رنگ) را انتخاب کنید. در صفحهٔ جدیدی که برای شما باز می‌شود و در قسمت بالای صفحه، گزینهٔ «ایجاد گروه» را انتخاب کنید.

۲ اطلاعات اولیه برای ساخت گروه را وارد کنید و اعضای اولیهٔ گروه را انتخاب کنید. شما می‌توانید یک یا چند نفراز مخاطبانتان را به‌عنوان اعضای اولیه گروه انتخاب کنید و یا اینکه فقط نام خودتان را به‌عنوان عضو اولیهٔ گروه ثبت کنید.

ویرایش نام و تصویر گروه در بله

برای تغییر نام گروه در بله این مراحل را انجام دهید:

۱ در بالای صفحهٔ گروه، روی نام گروه بزنید.

۲ در صفحهٔ باز شده، بالا سمت راست، روی سه‌نقطه بزنید.

۳ از میان گزینه‌ها «تغییر نام گروه» را انتخاب کنید.

اگر از نسخهٔ وب استفاده می‌کنید، برای تغییر نام گروه

۱ بالای صفحهٔ گروه، روی نام گروه کلیک کنید.

۲ در صفحهٔ باز شده، بالا سمت چپ، روی سه‌نقطه بزنید.

۳ از میان گزینه‌ها «ویرایش پروفایل گروه» را انتخاب کنید.

ویرایش تصویر گروه در بله با نسخهٔ اندروید

۱ بالای صفحهٔ گروه، روی نام گروه بزنید.

۲ در صفحهٔ بازشده، کنار تصویر گروه، روی عکس دوربین بزنید. در این قسمت می‌توانید عکس گروه را ویرایش کنید و اگر از نسخهٔ وب استفاده می‌کنید، بالای صفحهٔ گروه، روی نام گروه کلیک کنید.

۳ در صفحهٔ باز شده، بالا سمت چپ، روی سه‌نقطه بزنید.

۴ از میان گزینه‌ها «ویرایش پروفایل گروه» را انتخاب کنید و از قسمت «بارگذاری عکس گروه» تصویر را تغییر دهید.

خصوصی‌کردن گروه در بله با نسخهٔ اندروید

۱ بالای صفحهٔ گروه، روی نام گروه بزنید.

۲ در صفحهٔ باز شده، بالا سمت راست، روی سه‌نقطه بزنید.

۳ از میان گزینه‌ها «تبدیل به گروه خصوصی» را انتخاب کنید.

برای خصوصی کردن گروه در بله با نسخهٔ وب:

۱ بالای صفحهٔ گروه، روی نام گروه کلیک کنید.

۲ در صفحهٔ باز شده، بالا سمت چپ، روی علامت تنظیمات بزنید.

۳ از میان گزینه‌ها «نوع گروه» را انتخاب کنید و «گروه خصوصی» را علامت بزنید.

آموزش قفل کردن گروه

به‌عنوان مدیر یا مالک گروه، ممکن است زمان‌هایی نیاز داشته باشید که فعالیت افراد گروه را کنترل کنید. در این مواقع با قفل کردن یا به اصطلاح بستن گروه می‌توانید گروه را تا زمانی مشخص غیرفعال کرده و فعالیت

افراد گروه را کنترل کنید. چگونه در بله گروه را ببندیم یا قفل کنیم؟ برای قفل کردن گروه در بله باید مجوز ارسال پیام اعضای گروه را غیرفعال کنید. برای این کار، باید این مراحل را طی کنید:

۱ وارد گروه شوید.
۲ روی نام گروه بزنید.
۳ به بخش «اعضای گروه» بروید.
۴ «تعیین مجوز اعضا» را انتخاب کنید.
۵ بخش «ارسال پیام» را غیرفعال کنید.

برای بازکردن گروه و برگرداندن مجوز فعالیت، از همین مسیر به بخش «تعیین مجوز اعضا» بروید و امکان ارسال پیام را فعال کنید.

۳ـ۶ـ جرائم رایانه‌ای در شبکه‌های اجتماعی

با توسعه و پیشرفت تکنولوژی و نقش پررنگ آن در جوامع امروزی، این حوزه به‌صورت یک موضوع جدید و پرچالش تبدیل شده است. امروزه نمی‌توان تأثیر استفاده از اینترنت و وسایل الکترونیکی از جمله کامپیوترها و موبایل‌ها را بر زندگی افراد نادیده گرفت. حضور افراد در فضای مجازی، ایجاد کسب و کار در این فضا، شکل‌گیری روابط اجتماعی در آن و همچنین انجام معاملات تجاری از طریق آن باعث شده است این فضا به‌عنوان یک محیط مجازی درآید که برخی از افراد از آن سودجویی می‌کنند. از این رو قانون‌گذار برای جلوگیری از ایجاد اختلال در این فضا و مشخص کردن قواعد استفاده‌کنندگان، قوانینی را در این زمینه وضع کرده است.

درهر فضایی که افراد زیادی آنجا حضور دارند، احتمال وقوع جرم می‌رود. مشخص است که فضای مجازی از این قاعده مستثنی نیست و می‌دانیم که جرایم فضای مجازی کم نیستند. همان‌طورکه می‌دانیم، جرایم شبکه‌های اجتماعی و فضای مجازی متنوع هستند و جرایمی هم که در آنها اتفاق می‌افتد، طیف گسترده‌ای دارد. اما به‌طور کلی اینستاگرام و تلگرام، بیشترین آمار گزارش تخلف را به خود اختصاص داده‌اند.

جرایم شبکه‌های اجتماعی در سبک‌ها و مدل‌های مختلف اتفاق می‌افتد که در ادامه به برخی از آنها اشاره می‌کنیم:

۱ هک کردن حساب کاربران
۲ کلاهبرداری در فضای اینترنت
۳ جعل عنوان
۴ تجاوز به حریم شخصی آدم‌ها
۵ جرائم اقتصادی، اجتماعی و فرهنگی
۶ جرائم اخلاقی
۷ دزدیدن اطلاعات

شکل ۶ـ۶ـ سبک جرایم در شبکه‌های اجتماعی

مطالعه آزاد

برخی از جرایم، جرایم شبکه‌های اجتماعی محسوب می‌شوند که تعدادی از کاربران با آن مواجه می‌شوند. کمیته‌ای در قانون وجود دارد که مصادیق عینی جرم و جرایم شبکه‌های اجتماعی را مشخص می‌کند. این کمیته مصداق جرم را در جرایم شبکه‌های اجتماعی به‌طورکلی این‌گونه اعلام کرده است:

۱ ارائه محتوا برخلاف عفت عمومی
۲ ارائه محتوا علیه مقدسات
۳ ارائه محتوا علیه امنیت
۴ ارائه محتوایی علیه مقامات دولتی
۵ ارائه محتوایی که به ارتکاب جرم‌های رایانه‌ای کمک کند.

جزئیات این موارد قوانین جرایم شبکه‌های اجتماعی به شرح زیر مطرح شده است:

۱ بند ب ماده ۱۵ قانون جرائم رایانه‌ای و ماده ۶۳۹ قانون مجازات اسلامی: تشویق یا تهدید به فساد و فحشا
۲ بند۲ ماده ۶ قانون مطبوعات: ترویج فحشا
۳ ماده ۱۵ قانون جرائم رایانه‌ای: تشویق یا تهدید افراد برای دستیابی به محتوای مستهجن
۴ بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی: منتشرکردن هر مطلبی که مربوط به افترا زدن به مقامات و سازمان‌های حکومتی باشد.
۵ بند ۹ ماده ۶ قانون مطبوعات: تبلیغ کردن به نفع گروه‌های مخالف اسلام
۶ بند ج ماده ۲۵ قانون جرائم رایانه‌ای: منتشرکردن فیلترشکن و آموزش دادن استفاده از آن.
۷ ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵: تبلیغ و پخش مواد مخدر، سیگار و روان‌گردان
۸ ماده ۵۱۴ قانون مجازات اسلامی: اهانت‌کردن به امام‌خمینی (ره) یا تحریف آثار ایشان
۹ ماده ۱۵ قانون جرائم رایانه‌ای: منتشرکردن محتواهایی که به اعمال خشونت‌آمیز و خودکشی تشویق می‌کند
۱۰ بند ۱۰ ماده ۶ قانون مطبوعات: استفاده ابزاری از افراد، چه مرد باشد چه زن، در محتوا و تصویر
۱۱ ماده ۵۱۲ قانون مجازات اسلامی: تحریک‌کردن مردم برای کشتن یکدیگر
۱۲ بند ۶ ماده ۶ قانون مطبوعات: فاش‌کردن غیرمجاز اسرار نیروهای مسلح
۱۳ بند ۱۲ ماده ۶ قانون مطبوعات: منتشرکردن محتوا علیه قانون اساسی کشور
۱۴ بند ۷ ماده ۶ قانون مطبوعات: اهانت‌کردن به مقام معظم رهبری و سایر مراجع تقلید
۱۵ ماده ۲۱ قانون جرائم رایانه‌ای: آموزش دادن جرایم رایانه‌ای
۱۶ مواد ۶۸ و ۸۸ قانون انتخابات ریاست جمهوری: منتشرکردن هرگونه تبلیغات از سوی ارگان‌های دولتی له یا علیه نامزدهای انتخاباتی
۱۷ مواد ۶۹۷ و ۶۹۸ قانون مجازات اسلامی و بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی: انتشار اخبار کذب از فرایند انتخابات
۱۸ بند۷ ماده ۳۳ قانون انتخابات ریاست جمهوری ـ مواد ۵۰۰ و ۶۹۸ قانون مجازات اسلامی ـ بند ۴ ماده ۶ قانون مطبوعات ـ مصوبه شورای عالی امنیت ملی و ماده ۶۴ قانون انتخابات مجلس شورای اسلامی: تشویش اذهان عمومی و ایجاد اختلاف بین اعضای جامعه

جرایم شبکه‌های اجتماعی در اینستاگرام و واتساپ: اگر از جمله افرادی باشید که در این شبکه‌های اجتماعی صفحه دارید و در حوزه تخصصی خودتان فعالیت می‌کنید یا به بلاگری می‌پردازید، به احتمال زیاد با توهین و تهدید از جانب افراد مواجه شدید.

لازم است بدانید اگر از این موارد پرینت بگیرید، می‌توانید با مراجعه به دادسرای جرایم رایانه‌ای اعلام شکایت کنید. این شکایت از جانب پلیس فتا، از شناسایی مجرم تا جمع‌آوری مستندات و مدارک لازم و فرستادن آن به دادگاه پیگیری می‌شود.

شکل ۷ـ۶ـ مدل مفهومی جرایم در شبکه‌های اجتماعی

جرایم شبکه‌های اجتماعی در صفحات جعلی: علاوه بر توهین و تهدید و بی‌احترامی که جزء جرایم شبکه‌های اجتماعی است، اگر با پیج‌های فیکی که با عناوین مختلف مانند: شرکت در قرعه‌کشی، گرفتن جایزه، فروش کالا و خدمات و... کلاهبرداری هم مواجه شدید، بدانید و آگاه باشید که می‌توانید از طریق پلیس فتا پیگیری کنید.

اما گاهی کاربران به‌دلیل آنکه مبلغی که پرداخت کرده‌اند ناچیز بوده یا آن کالا و خدماتی که خریداری کرده بودند، غیرمجاز بوده است، از شکایت و پیگیری آن منصرف می‌شوند و همین باعث رشد بیشتر این شیادان می‌شود.

مجازات کسانی که به جرایم شبکه‌های اجتماعی مرتکب می‌شوند: همان‌طورکه می‌دانید برای هر جرمی مجازاتی وجود دارد، مثلاً اگر مزاحمت از طریق تلفن یا هر دستگاه مخابراتی انجام شود و به‌گونه‌ای باشد که برای فرد تهدید آبرویی، افشای اطلاعات شخصی، تهدید مالی و جانی باشد. حبس در ۲ ماه تا ۲ سال یا ۷۴ ضربه شلاق می‌باشد. اگر با استفاده از هویت کسی صفحه جعلی بسازند و از نام او سوء استفاده کنند، ۱ تا ۵ سال حبس و ۲۰ تا ۱۰۰ میلیون ریال جریمه در نظر گرفته می‌شود.

تحقیق

مجازات سوء استفاده از هویت دیگران در صفحات جعلی چیست؟

۱ـ۳ـ۶ـ کار با بخش‌های امنیتی شبکه‌های اجتماعی

افزایش امنیت در شبکه‌های اجتماعی

شکل ۸ـ۶

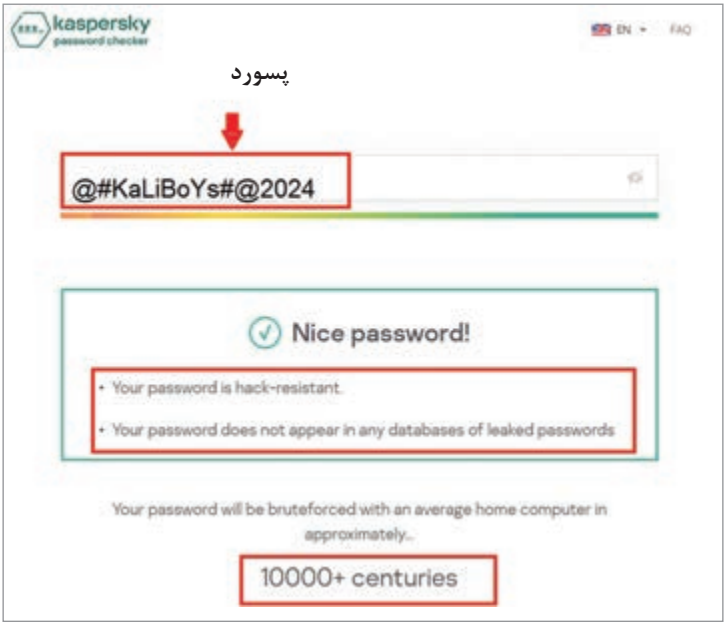
امروزه با پیشرفت تکنولوژی و روی کار آمدن اینترنت و فضای مجازی و همچنین پیوستگی مشاغل در شبکه‌های اجتماعی و بازدهی بالا، عموم مردم بیشتر اوقات خود را در رسانه‌های اجتماعی می‌گذرانند، از این‌رو خطرات امنیتی در رابطه با شبکه‌های اجتماعی افزایش می‌یابد. نکاتی که برای حفظ امنیت در شبکه‌های اجتماعی مطرح می‌شود:

۱ افزایش امنیت در سرویس‌های پست الکترونیک (Email)
۲ نحوه انتخاب بهترین گذرواژه
۳ افزایش امنیت در پیام‌رسان‌ها
۴ فقط به تنظیمات پیش‌فرض اکتفا نکنید.
۵ اگر مورد هک قرار گرفتیم چه کار کنیم؟

۱ـ افزایش امنیت در سرویس‌های پست الکترونیک (Email): امروزه هیچ سرویسی را نمی توانید پیدا کنید که برای عضویت در آن نیازی به سرویس پست الکترونیک یا همان ایمیل نباشد! با این حساب برای فعالیت در رسانه‌های اجتماعی و عضویت در آنها، حتماً باید یک سرویس ایمیل داشته باشیم که معروف‌ترین آنها Gmail و Email yahoo هستند که در اینجا می‌توانید با نحوه ساخت حساب کاربری در این دو سرویس آشنا شوید.
از این‌رو یکی از راه‌هایی که کسب و کار یا حساب‌های رسانه اجتماعی شما را به خطر می‌اندازد، پست الکترونیک شماست. پس بنابراین باید کاری کرد که ایمیل ما امنیت بالایی داشته باشد. برای این کار می‌توانید نکات زیر را رعایت کنید:

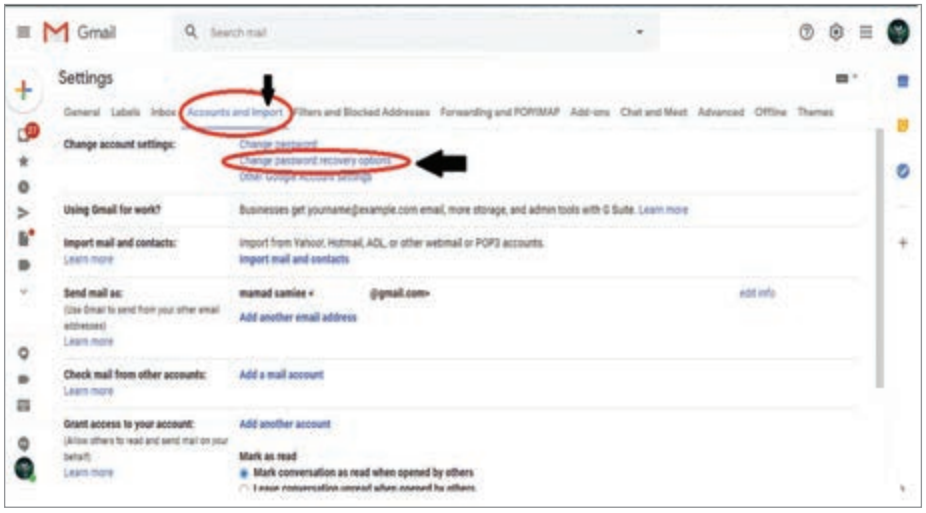
۱ استفاده از پسورد با ضریب قوی
۲ دو مرحله‌ای کردن تأیید ورود
۳ گذاشتن سؤالات امنیتی
۴ عدم دسترسی افراد به ایمیل

۱ـ استفاده از پسورد با ضریب قوی: مورد اول پسورد یا رمز عبور قوی است. برای تست و فهمیدن ضریب رمز عبور خود می‌توانید از قابلیتی که شرکت آنتی ویروسی کسپراسکای در اختیار شما می‌گذارد استفاده کنید! البته این را توصیه نمی‌توان کرد چون احتمال دارد یک دیتابیس از پسوردها را برای خود جمع‌آوری کنند!



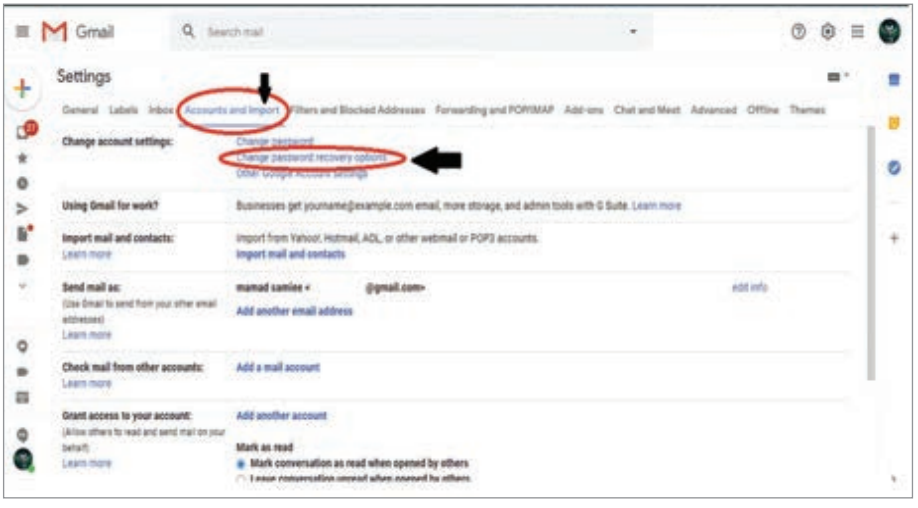
شکل ۹ـ۶ـ پنجره kaspersky

۲ـ نحوهٔ انتخاب بهترین گذرواژه: همان‌طور که در تصویر بالا مشاهده می‌کنید با استفاده از حروف بزرگ و کوچک، @ و # و اعداد توانستیم ضرب کرک پسورد خود را به ۱۰۰۰۰ قرن برسانیم!
نکته بعدی تأیید دو مرحله‌ای است که بعد از وارد کردن پسورد صحیح باید از طریق پیام کوتاه، ایمیل، تماس و یا پاپ آپ آمدن روی گوشی خود تأیید کنید که خودتان می‌خواهید وارد حساب ایمیل خود شوید.
برای فعال کردن تأیید دو مرحله‌ای Gmail می‌توانید به آدرس Settings >Accounts and Import >Change password recovery options رفته و تنظیمات آن را فعال کنید.



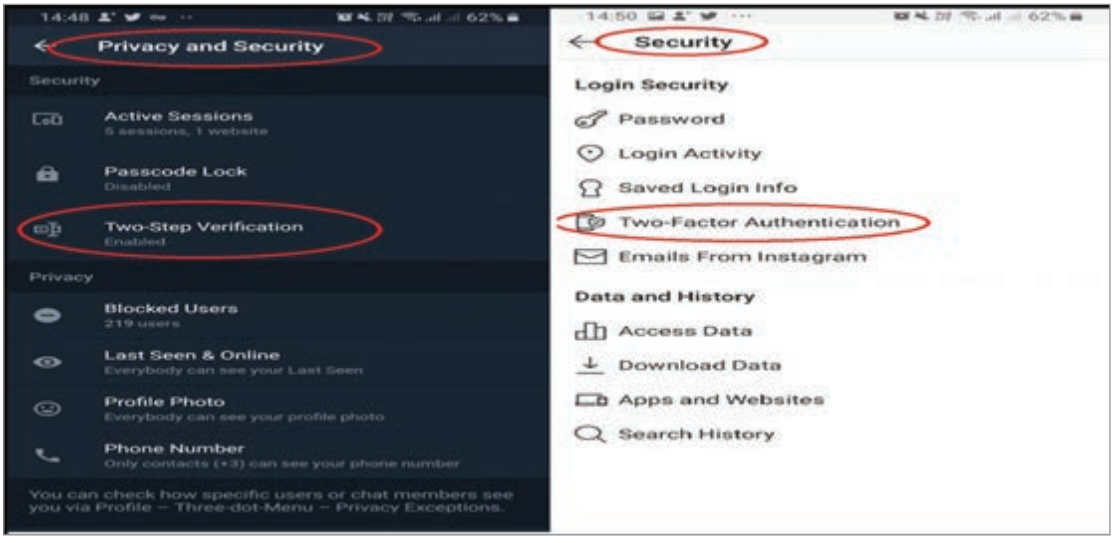
شکل ۱۰ـ۶

۲ـ دو مرحله‌ای کردن تأیید ورود: بعد از ورود به قسمت change password recovery options، همانند تصویر بالا می‌توانید با فعال کردن تأیید دو مرحله‌ای (2- step verification) و تنظیم شماره تماس بازیابی (Recovery phone) و ایمیل بازیابی (Recovery email) برای تأیید دو مرحله‌ای، Gmail خود را امن‌تر کنید.



شکل ۱۱ـ۶ـ تنظیم تأیید دو مرحله‌ای Gmail

۳ـ افزایش امنیت در پیام‌رسان‌ها: تأیید دو مرحله‌ای در پیام‌رسان‌ها هم مثل ایمیل می‌باشد، در اکثر پیام‌رسان‌ها می‌توانید از قسمت تنظیمات و بخش حریم خصوصی و امنیت (Privacy and Security)، تأیید دو مرحله‌ای را فعال کنید.
تصاویر بالا مربوط به تأیید دو مرحله‌ای در شبکه اجتماعی تلگرام و اینستاگرام می‌باشد.



شکل ۱۲ـ۶ـ افزایش امنیت در پیام‌رسان‌ها

۴ـ فقط به تنظیمات پیش‌فرض اکتفا نکنید: هنگامی که یک پروفایل رسانه اجتماعی ایجاد می‌کنید، به‌طور خودکار مطابق تنظیمات پیش‌فرض خود را تنظیم می‌کند. مشکلی که وجود دارد این است که اکثر این تنظیمات سست‌ترین استانداردهای امنیتی را در هر بستر رسانه اجتماعی مشخص نشان می‌دهند. به‌همین دلیل بسیار مهم است که تنظیمات حریم خصوصی حساب‌های رسانه‌های اجتماعی خود را به‌صورت دستی تنظیم‌کنید تا امنیت آنها به حداکثر برسد.
۵ـ اگر مورد هک قرار گرفتیم چه کار کنیم؟ حال مهم‌ترین بخش از افزایش امنیت در شبکه‌های اجتماعی، زمانی است که نکات امنیتی و حریم خصوصی را رعایت نکنیم. زمانی‌که یک هکر به حساب ما دسترسی پیدا می‌کند، سرعت ما باعث نجات ما می‌شود. در اکثر شبکه‌های اجتماعی زمانی‌که یک نفر دیگر به حساب ما ورود پیدا می‌کند، یک ایمیل و یا پیام کوتاهی مبنی بر ورود شخص دیگر برای ما ارسال می‌کند. در این صورت ما به‌راحتی می‌توانیم ورود شخص را به حساب خود مسدود کنیم.

۴ـ۶ـ اخلاقیات آنلاین، حفظ حریم خصوصی افراد و رعایت حقوق شهروندی

همان‌طورکه در یک جامعه شهروندان دارای حقوقی هستند، در فضای مجازی نیز کاربران حقوقی دارند که باید حفظ شده و با آنچه باعث نقض حقوق شهروندی می‌شود، مقابله شود.

شکل ۱۳ـ۶ـ مفهوم امنیت و حریم خصوصی

درواقع بین فضای سایبر و جامعه واقعی از این حیث که شهروندان دارای حقوقی هستند و باید این حقوق حفظ شود، فرقی وجود ندارد. با وجود این، در فضای مجازی ویژگی‌هایی است که آن را از جامعه واقعی متفاوت می‌کند و به همان نسبت هم حقوق کاربران در فضای سایبری دارای اهمیت بیشتری می‌شود. درحالی که در جامعه روی برخی از حقوق شهروندی تأکید بیشتری می‌شود که قانون‌گذار باید حمایت‌های فوق‌العاده‌ای نسبت به آن داشته باشد. در فضای سایبری هم حقوق کاربران اقتضای این را دارد که قانون‌گذار حمایت مؤثرتری از آن انجام دهد.

«حق حریم خصوصی» در منشور حقوق شهروندی چگونه تعریف شده است؟

«حق حریم خصوصی» نهمین بند از منشور حقوق شهروندی است که پس از بند «حق دسترسی به فضای مجازی» آمده است.

در بند نهم منشور حقوق شهروندی با عنوان «حق حریم خصوصی» چنین عنوان شده است:

ماده ۳۶ـ حق هر شهروند است که حریم خصوصی او محترم شناخته شود. محل سکونت، اماکن و اشیاء خصوصی و وسایل نقلیه شخصی از تفتیش و بازرسی مصون است، مگر به حکم قانون.

ماده ۳۷ـ تفتیش، گردآوری، پردازش، به‌کارگیری و افشای نامه‌ها اعم از الکترونیکی و غیرالکترونیکی، اطلاعات و داده‌های شخصی و نیز سایر مرسولات پستی و ارتباطات از راه دور نظیر ارتباطات تلفنی، نمابر، بی‌سیم و ارتباطات اینترنتی خصوصی و مانند اینها ممنوع است، مگر به موجب قانون.

ماده ۳۸ـ گردآوری و انتشار اطلاعات خصوصی شهروندان جز با رضایت آگاهانه یا به حکم قانون ممنوع است.

ماده ۳۹ـ حق شهروندان است که از اطلاعات شخصی آنها که نزد دستگاه‌ها و اشخاص حقیقی و حقوقی است، حفاظت و حراست شود. در اختیار قرار دادن و افشای اطلاعات شخصی افراد ممنوع است و در صورت لزوم به درخواست نهادهای قضایی و اداری صالح منحصراً در اختیار آنها قرار می‌گیرد. هیچ مقام و مسئولی حق ندارد بدون مجوز صریح قانونی، اطلاعات شخصی افراد را در اختیار دیگری قرار داده یا آنها را افشا کند.

ماده ۴۰ـ هرگونه بازرسی و تفتیش بدنی باید با رعایت قوانین، احترام لازم و با استفاده از روش‌ها و ابزار غیر اهانت‌آمیز و غیر آزاردهنده انجام شود. همچنین آزمایش‌ها و اقدامات پزشکی اجباری بدون مجوز قانونی ممنوع است.

ماده ۴۱ـ کنترل‌های صوتی و تصویری خلاف قانون در محیط‌های کار، اماکن عمومی، فروشگاه‌ها و سایر محیط‌های ارائه خدمت به عموم، ممنوع است.

ماده ۴۲ـ حق شهروندان است که حرمت و حریم خصوصی آنها در رسانه‌ها و تریبون‌ها رعایت شود. در صورت نقض حرمت افراد و ایجاد ضرر مادی یا معنوی، مرتکبین طبق مقررات قانونی مسئول و موظف به جبران خسارت می‌باشند.

حمایت قانون‌گذار از سرمایه‌های معنوی و حفظ حقوق غیرمالی شهروندی همچون حق حمایت، آزادی توأم با مسئولیت، امنیت، تعرض‌ناپذیری مکالمات و مکاتبات، آزادی اندیشه و بیان، مصونیت جان، مال، حیثیت، اعتبار و شخصیت افراد از تعرض ناروا، نامشروع و غیرقانونی در قانون اساسی از جمله در اصول ۲۱، ۲۲، ۲۳، ۲۵، ۲۸، ۳۸ و ۳۹ و نیز دیگر قوانین عادی منبعث از مبانی و قواعد فقهی و اصول کلی حقوقی، حکایت از اهمیت پاسداشت حرمت و کرامت انسانی و احترام به آزادی‌های مشروع افراد جامعه دارد. حق خلوت و رعایت حریم خصوصی انسان‌ها که به‌عنوان یکی از مصداق‌های مهم سرمایه معنوی انسانی مورد توجه نهادهای حاکمیتی داخلی و سازمان‌های بین‌المللی قرار گرفته و در اعلامیه جهانی حقوق بشر سازمان ملل متحد و نیز اعلامیه حقوق بشر اسلامی شناسایی و بر حفظ آن تأکید شده است، نیاز به بررسی تحلیلی و شناخت جایگاهش در عرصه فقه اسلامی و حقوق موضوعه دارد.

مفهوم و مصداق‌های حق خلوت و حریم خصوصی

حق خلوت یا به تعبیری، حق داشتن یک زندگی خصوصی، به‌عنوان یکی از حقوق اساسی شهروندان، ارتباط عمیقی با حفظ شأن، کرامت، شخصیت، استقلال فردی، توسعه روابط شخصی، گسترش صمیمیت و امنیت روانی پایدار و حاکمیت بر احساسات و افکار و دیگر ارزش‌های مهم انسانی دارد. حریم خصوصی در دو معنا قابل تصور است؛ معنای نخست آن به مفهوم حوزه خصوصی و تعرض‌ناپذیری حیات فردی انسان می‌باشد که معادل عبارت Private Domain در زبان انگلیسی است. حریم خصوصی در معنای دوم مبتنی بر حق افراد در مصون بودن از تعرض به حریم خصوصی‌شان به مفهوم اول است که همان بهره‌مندی از حریم خصوصی می‌باشد و معادل Privacy Right در زبان انگلیسی است. مفهوم اصطلاح حریم خصوصی همان تعریف حق خلوت است که برخی نویسندگان از آن به‌عنوان حق امنیت فردی، مصونیت مسکن و حیثیت و تعرض‌ناپذیری مکاتبات یاد نموده‌اند. حق خلوت عبارت است از «حق داشتن یک چارچوب محافظت شده، امن و خالی از اغیار که در آن به دور از مداخله و فشار دیگران، شخص آن طور که میل دارد، زندگی کند.» یکی از مهم‌ترین مباحث مربوط به حق خلوت، شناخت معیار و مصداق‌های آن است. به دیگر سخن، براساس چه معیار و قاعده‌ای می‌توان مصداق‌های حق خلوت را شناخت؟ در پاسخ باید گفت معیاری قابل پذیرش است که ناظر بر منافع فرد و جامعه باشد. گرچه در شناسایی مصداق‌های تحت شمول حق خلوت اختلاف نظر وجود دارد؛ اما چهار مصداق قابل ذکر است:

۱ ورود بدون اجازه و غیرقانونی به خلوت و حریم خصوصی دیگری مانند بازرسی و تفتیش جیب و کیف افراد

۲ تصاحب و استفاده از اسم، القاب، عناوین و اعتبار دیگری

۳ انتشار اسرار و وقایع خصوصی افراد مانند روابط زناشویی، امور پزشکی، نامه‌های شخصی، خصوصیت و ویژگی‌ها و عادات شخصی

۴ انتشار و افشای اطلاعات نادرست و انتساب آنها به یک شخص مانند نشر اکاذیب و افترا.

قطعنامه کنگره بین‌المللی حقوق‌دانان مصادیق تعرض به حق خلوت را چنین بیان نموده است:

۱ مداخله در زندگی داخلی و خانوادگی فرد

۲ تعرض به تمامیت جسمانی و روانی و ایجاد محدودیت‌های اخلاقی و معنوی

۳ تعرض به حیثیت، شرافت و شهرت فرد
۴ تفسیر مضر و نابجا از گفته‌ها و اعمال شخص
۵ افشای امور ناراحت‌کننده مربوط به زندگی خصوصی فرد
۶ استفاده از اسم، هویت و عکس دیگری برای مقاصد تجاری و تبلیغاتی
۷ تحت نظر قراردادن یا توقیف شخص و یا جاسوسی کردن درباره او
۸ بازرسی مکاتبات دیگری
۹ سوءاستفاده از مکاتبات کتبی یا شفاهی او
۱۰ افشای اطلاعاتی که از کسی در نتیجه ارتباط حرفه‌ای گرفته یا داده شده است؛ خلاف قاعده حفظ اسرار شغلی و حرفه‌ای.

اصل احترام به حق خلوت مانند هر اصل حقوقی دیگری در برخی موارد استثناپذیر است. در اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق مدنی و سیاسی، حفظ امنیت ملی، نظم عمومی، سلامت و اخلاق عمومی، حقوق و آزادی‌های دیگران، خطوط قرمز، حق خلوت ذکر شده است.

جرائم رایج رایانه‌ای و شبکه‌های اجتماعی

به‌طور کلی جرائم فضای مجازی به سه دسته کلی تقسیم‌بندی می‌شوند:
دسته اول: جرم از طریق دستگاه‌های هوشمند که نیاز به اینترنت ندارد.
دسته دوم: جرائمی می‌باشند که در نوع غیرمجازی نیز وجود دارند. مانند جعل و یا کلاهبرداری.
دسته سوم: جرائم سایبری نظیر هک، شنود، دست‌کاری داده‌های اینترنتی می‌باشد.

شکستن حرمت یا هتک حرمت

طبق ماده ۱۷ قانون جرایم رایانه‌ای، افرادی که با نشر مقاله‌های کاذب علیه یکدیگر اقدام به عمل هتک کرده، می‌بایست بعد از اثبات شدن جرمشان آماده پاسخگویی به قانون باشند و در نظر داشته باشند که این دسته از افراد نمی‌توانند از زیر بار مسئولیت اعمال خود فرار کنند. قوانین مرتبط با جرایم شبکه‌های اجتماعی را می‌توان در قوانین جرایم رایانه‌ای یافت.

محتوا علیه عفت و اخلاق عمومی

۱ تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشا و یا انحرافات جنسی (بند ب ماده ۱۵ قانون جرائم رایانه‌ای و ماده ۶۳۹ قانون مجازات اسلامی)
۲ اشاعه فحشاء و منکرات (بند۲ ماده۶ قانون مطبوعات)
۳ تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستهجن و مبتذل (ماده ۱۵ قانون جرائم رایانه‌ای)
۴ انتشار یا بازنشر هرگونه محتوا علیه امنیت و آسایش عمومی نیز در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد.
۵ انتشار یا بازنشر هرگونه محتوا علیه مقدسات اسلامی اعم از توهین، تبلیغ و به سخره گرفتن آن در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد.
۶ انتشار یا بازنشر هرگونه مطالب مرتبط افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی (بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی)
۷ تبلیغ به نفع حزب، گروه یا فرقه منحرف و مخالف اسلام (بند ۹ ماده ۶ قانون مطبوعات)
۸ انتشار فیلترشکن‌ها و آموزش روش‌های عبور از سامانه‌های فیلترینگ (بند ج ماده ۲۵ قانون جرائم رایانه‌ای)

۹ تبلیغ و ترویج مصرف مواد مخدر، مواد روان‌گردان و سیگار نیز در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد. (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵)

۱۰ اهانت به امام‌خمینی (ره) و تحریف آثار ایشان (ماده ۵۱۴ قانون مجازات اسلامی)

۱۱ انتشار و بازنشر محتوای حاوی تحریک، ترغیب، یا دعوت به اعمال خشونت‌آمیز و خودکشی نیز در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد. (ماده ۱۵ قانون جرائم رایانه‌ای)

۱۲ قانون جرایم رایانه‌ای برای هک‌کنندگان فضای مجازی ۲ سال حبس تعزیری و جریمه نقدی تعیین کرده است و درنظر داشته باشید برای مجازات افرادی که به‌صورت غیرمجاز به داده‌های اطلاعاتی افراد شامل صوت، تصویر یا متن گفت‌وگوها دستبرد بزنند حبس و جریمه نقدی تعیین کرده است.

۱۳ جالب است بدانید که قانون با تصویب قوانین جرائم رایانه‌ای به هیچ کس اجازهٔ تعرض به اطلاعات شخصی کسی را نداده حتی اگر این عمل ناپسند از طرف همسر آن شخص باشد.

۱۴ افشای اسرار خصوصی دیگران مطابق ماده ۷۴۵ قانون مجازات اسلامی و ماده ۱۶ قانون جرایم رایانه‌ای، چه به‌صورت عمدی و یا غیرعمدی شامل جریمه نقدی و تا دو سال حبس می‌باشد. باید در نظر داشته باشید که انتشار چت و اسکرین شات نیز می‌تواند شامل این قانون باشد.

۱۵ استفاده ابزاری از افراد (اعم از زن و مرد) در تصاویر و محتوا، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات نامشروع و غیرقانونی (بند ۱۰ ماده۶ قانون مطبوعات) تحریک یا اغوای مردم به جنگ و کشتار یکدیگر (ماده ۵۱۲ قانون مجازات اسلامی)

۱۶ فاش نمودن و انتشار غیرمجاز اسرار نیروهای مسلح در شبکه‌های مجازی نیز در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد. (بند ۶ ماده ۶ قانون مطبوعات)

۱۷ انتشار محتوا علیه اصول قانون اساسی در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد. (بند ۱۲ ماده ۶ قانون مطبوعات)

۱۸ اهانت به مقام معظم رهبری و سایر مراجع مسلم تقلید نیز در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد.(بند ۷ ماده ۶ قانون مطبوعات)

۱۹ آموزش و تسهیل جرائم رایانه‌ای (ماده ۲۱ قانون جرائم رایانه‌ای)

۲۰ انتشار و توزیع هرگونه محتوای تبلیغاتی از سوی کارکنان ادارات، سازمان‌ها، ارگان‌های دولتی و نهادها با ذکر سمت خود، له یا علیه هریک از نامزدهای انتخابات در فضای مجازی (مواد ۶۸ و ۸۸ قانون انتخابات ریاست جمهوری)

۲۱ انتشار اخبار کذب از نتایج بررسی صلاحیت‌ها، شمارش آراء، ادعاهای بی‌اساس پیرامون تقلب در انتخابات یا مخدوش‌بودن انتخابات بدون دلیل و مدرک (مواد ۶۹۷ و ۶۹۸ قانون مجازات اسلامی و بند ۸ ماده ۶۶ قانون انتخابات مجلس شورای اسلامی) در دسته جرایم شبکه‌های اجتماعی قرار می‌گیرد.

۲۲ این قانون بدین معنا می‌باشد که شما از یک سری کارها که بر عهده شما گذاشته شده یا از آن منع شده‌اید را انجام می‌دهید و در واقع خلاف آنچه بر شما مقرر شده عمل می‌کنید که این کار در قانون جرم شمرده شده است.

۲۳ تشویش اذهان عمومی، سیاه‌نمایی و بیان مطالب خلاف واقع علیه کشور، ایجاد اختلافات مابین اقشار جامعه به‌ویژه از طریق طرح مسائل قومی و نژادی، انتشار هرگونه نتایج نظرسازی و نظرسنجی کاذب در خصوص انتخابات و نامزدهای انتخاباتی (بند۷ ماده ۳۳ قانون انتخابات ریاست جمهوری ـ مواد ۵۰۰ و ۶۹۸

قانون مجازات اسلامی ـ بند ۴ ماده ۶ قانون مطبوعات ـ مصوبه شورای عالی امنیت ملی و ماده ۶۴ قانون انتخابات مجلس شورای اسلامی

اقدام به پیشگیری دولت به‌وسیله فیلترینگ

جالب است بدانیم که بیشترین شکایات و جرایم در این خصوص مربوط به تلگرام بوده و در جایگاه دوم اینستاگرام خودنمایی می‌کند. پس از اقدام به فیلتر شدن تلگرام باید درنظر داشت که شماره کاربران تلگرام تا حد زیادی کاهش پیدا کرده است. اما طبق سخنان رئیس پلیس فتا حدود ده تا دوازده میلیون نفر از فیلترشکن استفاده می‌کنند.

اینستاگرام به واسطه این‌که موضوع محور آن حول فایل‌های عکسی و فیلم است جلب توجه زیادی بین کاربران گوشی‌های هوشمند کرده و محبوبیت فراوانی بین کاربران دنیای اینترنت پیدا کرده و همچنین رقیب سرسختی برای دیگر شبکه‌های اجتماعی نظیر فیسبوک و توئیتر شده است؛ چرا که ماهیت توئیتر حول محور نوشته و فایل متنی می‌باشد. همین امر باعث شده تا توجه کلاهبرداران حوزهٔ مدلینگ به این نوع از جرائم شبکه اجتماعی جلب شده و فعالیت خود را گسترش بدهند.

رئیس پلیس فتا نیز در مورد برخی از موارد به هم‌میهنان عزیز هشدارهایی داده است: «باید در نظر داشت که احراز هویت در این شبکه‌ها امری سخت و بسیار مهم است؛ چرا که تعداد اکانت‌های فیک کم نمی‌باشد.»

فروشندگان کالای تقلبی

از دیگر کلاهبرداران فعال در زمینه جرایم شبکه‌های مجازی فروشندگان کالای تقلبی هستند. این اشخاص با گذاشتن عکس‌ها و فیلم‌هایی با جذابیت کاذب، بیننده را ترغیب به خرید و استفاده از آنها می‌کند. اگر شما و اطرافیانتان نیز یکی از کاربران این شبکه‌ها هستید به احتمال زیاد موارد مشابه از این قبیل جرائم یا تبلیغات فروش کالاهای غیراستاندارد را دیده یا به دام آنها افتاده‌اید. جالب است بدانید توهین، تهدید و مزاحمت در شبکه‌های اجتماعی می‌تواند پیگیری شود و پلیس فتا پیگیری آنها را با دقت انجام می‌دهد.

فحاشی در فضای مجازی

یکی دیگر از ناهنجاری‌های رایج در فضای مجازی توهین، فحاشی و ناسزاگویی می‌باشد که متأسفانه بی‌اطلاعی مردمی که مورد توهین قرار می‌گیرند از حقوق قانونی خود و عدم برخورد قانونی با چنین افرادی، زمینه را برای ایجاد چنین جرمی برای افرادی فراهم می‌کند. در حالی‌که مطابق با قانون مجازات اسلامی، طبق مواد ۱۴۵ و ۶۰۸، این اعمال قبیح (فحاشی، توهین، هتاکی و...) را «جرم انگاری» کرده و «جزای نقدی از یک تا پنجاه میلیون ریال» یا «۷۴ ضربه شلاق» برای مجازات مجرمان در نظر گرفته است.

خلاصه مطالب فصل ۶

- شبکه اجتماعی: ساختاری اجتماعی است که از گروه‌هایی (عموماً فردی یا سازمانی) تشکیل شده‌است که توسط یک یا چند نوع خاص از وابستگی مانند ایده‌ها و تبادلات مالی، دوستان، خویشاوندان، لینک‌های وب، به هم وصل هستند.
- رسانه اجتماعی مجازی: عبارت است از بسترهای مبتنی بر فناوری که زمینه ارتباط، تعامل و گردهمایی برای تولید و مصرف محتوا را فراهم می‌کنند.
- انواع شبکه‌های اجتماعی شامل: تصویرمحور: به‌عنوان مثال از لحاظ محتوا، شبکه اینستاگرام تصویر محور است و ویدیو محور: مانند تیک‌تاک و گفت‌وگو محور: مانند Reddit و Quora و شبکه‌های اجتماعی وبلاگی و انجمن.
- جهت افزایش امنیت در سرویس‌های پست الکترونیک رعایت نکات زیر ضروری است:

استفاده از پسورد با ضریب قوی، دو مرحله‌ای کردن تأیید ورود، گذاشتن سؤالات امنیتی، عدم دسترسی افراد به ایمیل.

- جرایم شبکه‌های اجتماعی در سبک‌ها و مدل‌ها مختلف شامل: هک کردن حساب کاربران، کلاهبرداری در فضای اینترنت، جعل عنوان، تجاوز به حریم شخصی آدم‌ها، جرائم اقتصادی، اجتماعی و فرهنگی، جرائم اخلاقی، دزدیدن اطلاعات است.
- حق حریم خصوصی افراد یعنی:

ـ حریم خصوصی او محترم شناخته شود. محل سکونت، اماکن و اشیاء خصوصی و وسایل نقلیه شخصی از تفتیش و بازرسی مصون است، مگر به حکم قانون.

ـ تفتیش، گردآوری، پردازش، به‌کارگیری و افشای نامه‌ها اعم از الکترونیکی و غیرالکترونیکی، اطلاعات و داده‌های شخصی و نیز سایر مرسولات پستی و ارتباطات از راه دور نظیر ارتباطات تلفنی، نمابر، بی‌سیم و ارتباطات اینترنتی خصوصی و مانند اینها ممنوع است، مگر به موجب قانون.

ـ گردآوری و انتشار اطلاعات خصوصی شهروندان جز با رضایت آگاهانه یا به حکم قانون ممنوع است.

ـ هیچ مقام و مسئولی حق ندارد بدون مجوز صریح قانونی، اطلاعات شخصی افراد را در اختیار دیگری قرار داده یا آنها را افشا کند.

ـ کنترل‌های صوتی و تصویری خلاف قانون در محیط‌های کار، اماکن عمومی، فروشگاه‌ها و سایر محیط‌های ارائه خدمت به عموم، ممنوع است.

- جرائم رایج رایانه‌ای و شبکه‌های اجتماعی سه دسته می‌باشد:

دسته اول: جرم از طریق دستگاه‌های هوشمند که نیاز به اینترنت ندارد.

دسته دوم: جرائمی می‌باشند که در نوع غیرمجازی نیز وجود دارند. مانند جعل و یا کلاهبرداری.

دسته سوم: جرائمی سایبری نظیر هک، شنود، دستکاری داده‌های اینترنتی می‌باشد.

پرسش‌های چهارگزینه‌ای

۱ نخستین بار مفهومی با عنوان شبکه‌های اجتماعی اینترنتی در چه سالی و در کدام کشور مطرح شد؟
الف) آلمان ۱۹۹۰ ب) آمریکا ۱۹۶۰ ج) انگلیس ۱۹۹۰ د) فرانسه ۱۹۶۰

۲ کدام موارد زیر از مهم‌ترین اهداف شبکه‌های اجتماعی است؟
الف) ایجاد یک پایگاه داده از کاربران ب) ایجاد رفاه و امکانات بیشتر
ج) به‌وجود آمدن نوعی عدالت و برابری د) همه موارد

۳ کدام یک جزء شبکه‌های اجتماعی مجازی نیست؟
الف) شبکه‌های اجتماعی نوشتار محور ب) شبکه‌های اجتماعی گفتار محور
ج) شبکه‌های اجتماعی تصویر محور د) شبکه‌های اجتماعی ویدیو محور

۴ کدام شبکه‌های اجتماعی ایرانی است که علاوه بر ارسال پیام به انجام امور مالی نیز می‌پردازد؟
الف) ایتا ب) روبیکا ج) بله د) آی‌گپ

۵ کدام گزینه زیر به معنی مستقیم و بدون واسطه می‌باشد؟
الف) Direct ب) Forward ج) Pin د) Post

۶ کدام‌یک جزء شبکه اجتماعی مبتنی بر اشتراک‌گذاری تصویر و ویدیو از سایت‌های دیگر است؟
الف) فیسبوک ب) اینستاگرام ج) پینترست د) توییتر

۷ جرایم شبکه‌های اجتماعی در کدام یک از سبک‌ها و مدل‌های زیر اتفاق می‌افتد؟
الف)هک کردن حساب کاربران ب) جعل عنوان
ج) جرائم اخلاقی د) هر سه مورد

۸ جعل و کلاهبرداری جزء کدام یک از جرایم فضای مجازی است؟
الف) دسته اول ب) دسته دوم ج) دسته سوم د) هر سه دسته