ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

شماره مجوز مجله: ۸۰۴۰۰ زمان چاپ: ۱۴۰۲/۱۲/۲۰

راهکارهای عملی برای کاهش انزوای اجتماعی دانش‌آموزان در دنیای مجازی

میترا نخعی

کارشناسی ارشد روانشناسی بالینی دانشگاه آزاد اسلامی واحد زنجان

چکیده

با گسترش روزافزون دنیای مجازی، حضور دانش‌آموزان در این فضا نیز افزایش یافته است. در حالی که دنیای مجازی فرصت‌های جدیدی برای یادگیری و تعامل ایجاد می‌کند، اما می‌تواند منجر به انزوای اجتماعی دانش‌آموزان نیز شود. انزوای اجتماعی، پیامدهای منفی متعددی برای سلامت روان و پیشرفت تحصیلی دانش‌آموزان دارد. با توجه به شیوع انزوای اجتماعی در بین دانش‌آموزان در دنیای مجازی، یافتن راهکارهای عملی برای کاهش این پدیده، از اهمیت بالایی برخوردار است. این راهکارها باید به گونه‌ای باشند که به دانش‌آموزان در برقراری ارتباطات اجتماعی سالم و مؤثر در دنیای مجازی کمک کنند. کاهش انزوای اجتماعی دانش‌آموزان در دنیای مجازی، فواید متعددی برای سلامت روان، پیشرفت تحصیلی و مهارت‌های اجتماعی آنها دارد. این امر به دانش‌آموزان کمک می‌کند تا روابط سالم و معناداری با دیگران برقرار کنند، از مزایای یادگیری اجتماعی بهره‌مند شوند و در دنیای واقعی نیز به طور فعال و مؤثر حضور داشته باشند. این مقاله به بررسی راهکارهای عملی برای کاهش انزوای اجتماعی دانش‌آموزان در دنیای مجازی می‌پردازد. با استفاده از راهکارهای ارائه شده در این مقاله، می‌توان به طور مؤثری انزوای اجتماعی دانش‌آموزان در دنیای مجازی را کاهش داد و به آنها کمک کرد تا از مزایای این فضا به طور صحیح و اصولی بهره‌مند شوند.

کلمات کلیدی: انزوای اجتماعی، دانش‌آموزان، دنیای مجازی، راهکارهای عملی، آموزش.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

مقدمه

با پیشرفت روزافزون فناوری و گسترش دنیای مجازی، شبکه‌های اجتماعی به عنوان یک بعد اساسی از زندگی مدرن جامعه به‌شمار می‌آیند. این شبکه‌ها، امکان ارتباطات گسترده و اشتراک‌گذاری تجربیات را فراهم ساخته و به دانش‌آموزان فرصتی برای ارتباط با همکلاسی‌ها و دیگر افراد فراهم می‌کنند. با این وجود، در کنار مزایا، موضوع انزوای اجتماعی در دانش‌آموزان به عنوان یک چالش مهم به چشم می‌آید. انزوای اجتماعی در دانش‌آموزان، با وجود فراهم شدن زیرساخت‌های ارتباطی از طریق شبکه‌های اجتماعی، به‌عنوان یک احساس معمول و گاهی ناخوشایند، در جامعه تحصیلی و اجتماعی پدیدار می‌شود. این مسأله می‌تواند بر روحیه، عملکرد تحصیلی، و به‌طور کلی، کیفیت زندگی تحصیلی دانش‌آموزان تأثیرگذار باشد.

امروزه بسیاری از مخاطبان اینترنتی به طور مداوم از تعداد زیادی از سایت های اجتماعی بازدید می کنند تا به ارتباط با همراهان خود ادامه دهند، افکار، عکس ها، ضبط های خود را به اشتراک بگذارند و حتی در مورد زندگی روزمره خود صحبت کنند. شبکه‌های اجتماعی را می‌توان به ایمیل اصلی که در سال ۱۹۷۱ ارسال شد، دنبال کرد، جایی که دو رایانه شخصی در کنار یکدیگر قرار داشتند. در سال ۱۹۸۷ سیستم تابلوی اعلانات اطلاعات را از طریق خطوط تلفن با مشتریان مختلف رد و بدل کرد و در اواخر همان سال، نسخه‌های اصلی برنامه‌های وب اولیه منتقل شد. [۱]. تعداد زیادی از مقاصد شبکه های اجتماعی و مکان های دنیای مجازی وجود دارد که حتی موتور جستجو برای آنها وجود دارد علاوه بر این، سایت های خاصی وجود دارد که مخاطبان را قادر می سازد تا وب سایت های شبکه اجتماعی خود را ایجاد کنند. این سایت های اجتماعی اثرات سازنده و منفی دارند. چنین تعداد زیادی از مردم بیشتر وقت خود را برای استفاده از این سایت ها تلف می کنند که باعث از دست دادن شغل یا دانشگاه یا حتی زندگی عادی اجتماعی و خانواده خود می شود! بسیاری دیگر مطالب دارای حق چاپ را بدون مجوز، محتوای مستهجن یا ممنوع ارسال می کنند. نوجوانان امروزه یکی از بزرگترین گروه های کاربران اینترنت هستند. نوجوانان کاربران اینترنت شامل دانش‌آموزان هستند. فعالیت های دانش آموزان در اینترنت به زندگی روزمره و نیاز آنها تبدیل شده است. متأسفانه، این دانش آموزان به طور کامل در مورد امنیت شخصی در فعالیت های مرتبط با اینترنت نمی دانند. بخشی از کاربران، کاربران باهوش، از سایت های شبکه های اجتماعی به صورت مثبت استفاده می کنند. همانطور که اکنون در بهار کل جهان اتفاق می افتد. در شرایط کنونی اکثر افراد، سازمان ها و کشورها وابستگی زیادی به انجام فعالیت های روزانه خود به اتصال به اینترنت دارند. امروزه اینترنت می تواند جهان را فوراً متصل کند. افرادی که از مکان‌های مختلف در منطقه زمانی مختلف متصل هستند، می‌توانند با اتصال به اینترنت با هم کار کنند، همکاری کنند و بحث کنند. علاوه بر این، دولت همچنین فعالیت های خود را از طریق اتصال به اینترنت انجام می دهد. همچنین به عنوان دولت الکترونیک شناخته می شود. با این حال، اگرچه دنیای مجازی امکانات متنوع و فرصت‌های بسیار زیادی را ارائه می‌دهد، از سوی دیگر، مردم متوجه نمی‌شوند که استفاده از اینترنت خطراتی دارد [۱].

کاربران اینترنت که از وای فا در مکان های عمومی برای اهداف تجاری یا خصوصی استفاده می کنند، باید مراقب امنیت اطلاعات شخصی خود باشند. اطلاعات و داده های شخصی کاربران که از طریق اتصال به اینترنت یا شبکه اینترنت پردازش می شوند، کاملاً ایمن نبودند [۲]. فرصتی وجود دارد که به دلیل رفتار بی دقتی آنها در استفاده از اینترنت، اطلاعات یا داده های خصوصی آنها محافظت نشده و همچنین هدف مجرمان سایبری برای انجام کارهایی قرار می گیرد که سازمان یا شرکت را به

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

خطر می اندازد [۳]. از این رو کشورهای مختلف آگاهی از امنیت سایبری را توسعه و پیاده سازی کرده اند و همچنین برنامه هایی را برای آموزش کاربران اینترنت در مورد اهمیت امنیت در فعالیت های اتصال به اینترنت ایجاد کرده اند [۴].

پشتیبانی از طیف گسترده‌تر خدمات اینترنتی و همچنین قیمت ارزان دستگاه‌های پشتیبانی از اینترنت مانند گوشی‌های هوشمند، رایانه‌های شخصی، تبلت‌ها، لپ‌تاپ‌ها و غیره باعث می‌شود کاربران دستگاه‌های فناوری اطلاعات به سرعت در اندونزی رشد کنند [۵]. با افزایش روزافزون کاربران اینترنت، تعداد جرایم سایبری در اندونزی پس از ژاپن در رتبه دوم جهان قرار دارد. [۶].

دانش آموزان هم از جمله مخاطبان و کاربران اصلی رسانه ها و شبکه های اجتماعی هستند که می توانند از دنیای مجازی برا رسیدن به موفقیت و اهداف آموزشی خود استفاده نمایند . آنها می توانند تحت نظارت معلمان و والدین خود به این شبکه ها دسترسی داشته باشند . اما امروزه استفاده های مضر از رسانه ها یا اجتماعی توسط دانش آموزان بیشتر از استفاده های مفید آنان است.ر معمولاً دانش آموزان هنگام استفاده از خدمات شبکه های اجتماعی مرتکب خطرات و خطاهای متعددی می شوند، به عنوان مثال، استفاده از برنامه های تأیید نشده، سوء استفاده از رایانه های شخصی شرکتی، دسترسی فیزیکی و شبکه تأیید نشده، سوء استفاده از رمزهای عبور و تبادل داده های حساس بین کار و رایانه هنگام کار در خانه است [۳].

شهرت اصطلاح سایت های شبکه های اجتماعی از سال ۱۹۹۷ گسترش یافته است و تعداد زیادی از مردم در حال حاضر از سایت های شبکه های اجتماعی برای صحبت با همراهان خود، انجام کارهای تجاری و استفاده های مختلف مختلف بر اساس علاقه کاربران استفاده می کنند.

شور و شوق سایت های شبکه های اجتماعی گسترش یافته و مقالات تحقیقاتی متعددی توزیع شده است. برخی از آنها به بررسی مسائل امنیتی شبکه های اجتماعی، بررسی حریم خصوصی و تهدید سایت های شبکه های اجتماعی آنلاین پرداختند. به طور کلی، یک شبکه اجتماعی یک ساختار اجتماعی است که از افراد یا انجمن هایی تشکیل شده است که حداقل توسط یک نوع خاص از وابستگی متقابل به هم مرتبط هستند، به عنوان مثال، مشارکت، علاقه عادی، و انتقال سرمایه، پیوندهای اعتقادی، یادگیری یا احترام. شبکه‌های اجتماعی را نیز می‌توان به عنوان آن دسته از سایت‌هایی توصیف کرد که افراد را قادر می‌سازد تا مبادلات آنلاین را چارچوب‌بندی کنند و طیف وسیعی از اطلاعات را مبادله کنند[۴].

امنیت سایبری به دلیل افزایش اتکا به تجهیزات و برنامه های دیجیتال برای مدیریت زندگی روزمره ما، از جمله انتقال و ذخیره اطلاعات شخصی، از اهمیت فزاینده ای برخوردار است. این دنیای دیجیتال امکانات بسیاری را فراهم می کند، اما خطرات جدیدی را نیز به همراه دارد که اغلب ناشناخته یا نادیده گرفته می شوند. سرعت رشد اینترنت از انتظارات و پیش بینی های توسعه دهندگان اولیه اینترنت فراتر رفت . شاید همین رشد سریع و غیرمنتظره اینترنت است که کاربران را در مورد مسائل امنیت سایبری در تاریکی قرار داده است. ما (جامعه) به اندازه کافی سریع آموزش در مورد دنیای مجازی را برنامه ریزی، ایجاد و انتشار ندادیم تا با افزایش استفاده از دنیای مجازی مطابقت داشته باشیم. در نتیجه، کاربران معمولی اینترنت/فناوری (از جمله دانشجویان فعلی کالج، که بیشتر آنها در دنیای سایبری بزرگ شده‌اند) از خطرات ایمنی و اطلاعات شخصی خود از طریق استفاده از وسایل الکترونیکی به روش‌های ناامن بی‌خبر هستندبه طور غیرمستقیم، این کاربران سنگین دستگاه های دیجیتال هستند که معمولاً کمترین دانش و آگاهی از مسائل امنیتی سایبری و پیشگیری را دارند. اگرچه نگرانی در مورد حفاظت از بدن

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

فیزیکی، دارایی و فضای خود برای اکثر مردم طبیعی است، نگرانی در مورد حفاظت از اطلاعات و دارایی خود در فضای سایبری طبیعی نیست. [۴].

این مقاله با هدف بررسی و ارائه راهکارهایی برای کاهش انزوای اجتماعی در دانش‌آموزان در شبکه‌های اجتماعی تدوین شده است. با توجه به اینکه انزوای اجتماعی می‌تواند به عنوان یک عامل موثر در کاهش عزت‌نفس و تحصیلات دانش‌آموزان تأثیر بگذارد، ارائه راهکارهای علمی و کاربردی جهت افزایش ارتباطات اجتماعی و کاهش احساس انزوای اجتماعی از اهمیت ویژه‌ای برخوردار است. این مقاله نه‌تنها به محققان و متخصصان علوم تربیتی، بلکه به مدیران مدارس و والدین نیز کمک خواهد کرد تا با استفاده از راهکارهای ارائه شده، محیطی حمایتی و دوستانه در شبکه‌های اجتماعی برای دانش‌آموزان فراهم آورند.

آسیب های شبکه‌های اجتماعی

اخیراً، شبکه‌های اجتماعی هزاران دانش آموز را جذب می‌کنند و پس از جذب کردن آنها را قربانی اهداف ناپسند خود می کنند[۳]. مهاجمان فضایهای مجازی که اکثر همسن خود دانش آموزان هستند برای شروع با فیش‌ها و هرزنامه‌هایی که از شبکه‌های اجتماعی برای ارسال پیام‌های جعلی به قربانیان «دوست» استفاده می‌کنند، مجرمان سایبری و کلاهبردارانی که از شبکه‌های اجتماعی برای گرفتن اطلاعات قربانیان در آن نقطه استفاده می‌کنند و حملات اجتماعی و تجمع‌های تروریستی خود را تکمیل می‌کنند. آسی های سایبری که ممکن است دانش آموزان با آن مواجه شوند را می توان به دو دسته طبقه بندی کرد[۴].

الف) آسیب های مربوط به حریم خصوصی

نگرانی‌های مربوط به حریم خصوصی از پروفایل‌های کاربر درخواست می‌کند که هرگز داده‌ها را در وب توزیع و پخش نکنند. مجموعه ای از داده ها در صفحات اصلی فردی ممکن است حاوی اطلاعات بسیار شخصی باشد، به عنوان مثال، تاریخ تولد، محل سکونت، و شماره سلول های فردی و غیره. این داده ها می تواند توسط هکرهایی که از استراتژی های طراحی اجتماعی برای به دست آوردن مزایای چنین داده های ظریف و گرفتن پول نقد استفاده می کنند، استفاده شود. دانش آموزان زمانی که برای کسب اطلاعات درسی خود به سایت های ناشناخته و مبهم وارد می شوند در ابتدای امر جهت دسترسی به اطلاعات مورد نظر خود تمامی اطلاعات خصوصی خود را تحت عنوان داده وارد می کنند و مهاجمان نیز از اطلاعات آنان سواستفاده می کنند. در فعالیت‌های دنیای مجازی، مجرمان جرایم سایبری از نقاط ضعف کاربران اینترنت که نوجوانان به‌ویژه دانش‌آموزان در سنین پایین‌تر هستند، هستند. این مجرمان از داده ها یا اطلاعات شخصی دانش آموزانی استفاده می کنند که از خطری که می تواند بر خود کاربر دانش آموز تأثیر بگذارد و همچنین سازمان یا مؤسسه کاربران را تحت تأثیر قرار دهد، بی اطلاع هستند.

پلتفرم های مدرن گوشی های هوشمند کاربردهای مختلفی دارند. به معنای درخواست مجوز برای دسترسی به داده ها و منابع شخصی، مانند حساب ایمیل، دوربین، مخاطبین یا مکان فعلی کاربر. کاربران گوشی های هوشمند دارنده کنترل این مجوز هستند. آنها باید متوجه شوند که مجوز دسترسی به اطلاعات خصوصی همیشه نباید تأیید شود.

کاربران برای انجام فعالیت در دنیای مجازی به یک اپلیکیشن نیاز دارند. این برنامه بر روی کامپیوتر یا تلفن همراه نصب شده است. همانطور که می دانیم اگر نصب برنامه را انجام دهیم، توافق کاربر در مورد برنامه وجود خواهد داشت. هنوز هم بسیاری از کاربران این برنامه ها هستند که هنگام نصب برنامه، قرارداد کاربر را نادیده می گیرند یا نمی خوانند. یکی از دلایل همه این

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

واقعیت این است که در قرارداد کاربر گاهی اوقات کلمات دشواری برای درک وجود دارد. کاربران تمایل دارند بدون نگرانی از دانستن اهداف و اهداف دقیق این برنامه‌ها، حتی خطر نصب برنامه‌ای که به طور رسمی با رضایت کاربران نصب شده است، «کلیک می‌کنم» می‌پذیرم/موافقم [۷].

در مورد مفهوم نظارت تصویری برای کاربران جوان اینترنت مانند وضعیت امتحان، در برخی از موسسات آموزشی رایج و رایج شده است. تاثیر مثبت نظارت تصویری در معاینه مانند راحتی کمیته امتحان برای اطمینان از اینکه امتحان به خوبی بدون هیچ گونه تقلب در امتحان برگزار می شود. از طرفی استفاده از دوربین مداربسته تاثیر منفی دارد ر شرایط امتحان به عنوان مثال، دانش آموزان در امتحان دچار عدم اعتماد به نفس، اعتماد به نفس پایین، احساس سوء ظن در بین آنها می شوند [۸].

تحقیق در مورد واکنش مردم در استفاده از نظارت دوربینی که منجر به نظارت دوربین یا آنلاین می شود که باعث ایجاد احساس بالاتری از نقض حریم خصوصی و فشار موقعیتی می شود. با آگاهی از نظارت، پاسخ دهندگان در تحقیق متوجه می شوند که اطلاعاتی که به صورت آنلاین به اشتراک می گذارند، در معرض دید سایر ناظران ناشناخته قرار می گیرد. علاوه بر این، این مورد می تواند قربانی ذخیره و اشتراک گذاری شود که منجر به تجاوز به حریم خصوصی می شود [۹].

استفاده از فناوری اینترنت در بین نوجوانان به ویژه دانش آموزان مدارس در انجام فعالیت های آموزشی جدایی ناپذیر است. با این حال، تهدیدات جرایم سایبری و همچنین استفاده از امنیت اطلاعات شخصی وجود دارد [۱۰]. این تهدید با افزایش تعداد کاربران اینترنت به طور قابل توجهی افزایش می یابد. بنابراین، امنیت سایبری یا پروتکل امنیتی در انجام اتصال به فضای سایبری نکته بسیار مهمی برای درک است. این به این دلیل است که در واقع امنیت سایبری به دور است یا تلاش برای محافظت از سخت افزار، نرم افزار، داده ها یا سیستم ها در برابر مجرمان در فضای سایبری است. [۱۱].

ب) آسیب های شبکه های سنتی

به طور کلی، دو نوع مسئله امنیتی وجود دارد: یکی امنیت افراد است. دیگری امنیت رایانه های شخصی است که افراد از آنها استفاده می کنند و اطلاعاتی که در سیستم خود ذخیره می کنند. از آنجایی که شبکه‌های اجتماعی تعداد زیادی مشتری دارند و حجم عظیمی از اطلاعات را در خود ذخیره می‌کنند، هدف منظمی برای ارسال‌کنندگان هرزنامه، فیشینگ و حملات بدخواهانه هستند. علاوه بر این، هکرهای اجتماعی آنلاین کلاهبرداری عمده، فیشینگ و حملات نفرت انگیز و آسیب به احترام فردی و قلدری سایبری را شامل می شوند. هکرها پروفایل های جعلی ایجاد می کنند و هویت ها یا علائم را کپی می کنند یا برای بدنام کردن یک فرد شناخته شده در داخل شبکه ای از همراهان از آنها استفاده می کنند . دانش آموزان براثر اختلافاتی که با همسالان خود دارند گاهی برای گرفتن انتقام و خالی کردن خشم خود شروع به تخریب شخصیت وی و بد نام کردن او در بین همسالان خود می کنند . آنها از قربانی های خود عکس های نابهنجار در دنیای مجازی به اشتراک می گذارند و یا از اطلاعات قربانیان استفاده می کنند و از طرف آنان به سایر دوستان خود پیام های نامطلوب میفرستند واینگونه وجه و شخصیت و امنیت قربانی را به خطر می اندازند [۱۱].

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

دانش امنیت سایبری دانش آموزان

این واقعیت نیاز به اجتماعی شدن درک امنیت سایبری را در بین کاربران اینترنت به ویژه جوانان از جمله دانش آموزان در مدرسه ایجاد می کند. دانستن سطح درک آنها و همچنین میزان نگرانی آنها در حفظ امنیت به ویژه در اشتراک گذاری اطلاعات به ویژه مسائل خصوصی و شخصی در دنیای مجازی بسیار مهم است [۱۲].

آموزش امنیت سایبری در مدرسه به بخش بسیار مهمی از فناوری اطلاعات تبدیل شده است که به طور گسترده توسط مدرسه مورد استفاده قرار گرفته است. استفاده از فناوری اطلاعات در مدارس شامل انجام یادگیری و تدریس، مدیریت مالی و اداره کل در سطح مدرسه. اهمیت آگاهی یا دانش در مورد امنیت سایبری نه تنها بر عهده کارکنان فناوری اطلاعات یا فقط چند نفر در مدرسه بلکه همه افراد درگیر است. افراد درگیر در آگاهی از امنیت سایبری از جمله معلمان، دانش آموزان و همه کارکنان. که دو نیم دانش کافی در مورد امنیت سایبری دارد زیرا این دانش یک مهارت بسیار مفید در زندگی روزمره است. این به این دلیل است که زندگی آنها در حال حاضر بخشی از زندگی جامعه دیجیتال است [۱۳].

یادگیری امنیت سایبری تنها اجرای یک برنامه درسی یا یک موضوع خاص در مدرسه نیست. علاوه بر این، مهمترین چیز افزایش آگاهی آنها است که زندگی در جامعه دیجیتال نیاز به سطحی از درک امنیت سایبری دارد. آنها که در جامعه دیجیتال زندگی می کنند، تقریباً هر روز به دنیای اینترنت متصل هستند و انواع مختلفی از اطلاعات را در مورد آن به اشتراک می گذارند. بنابراین باید میزان تمایل دانش آموزان را بدانیم که آیا معلمان به اجتماعی شدن دانش امنیت سایبری نیاز دارند [۱۴].

در برخی مدارس، آموزش امنیت سایبری اجباری می شود و همچنین برای دانش آموزان انتخابی می شود تا در مورد آن بیاموزند. در برنامه درسی، امنیت سایبری نه تنها در این کلاس ها در مورد خود امنیت سایبری، بلکه در مورد اخلاق سایبری و ایمنی سایبری نیز گنجانده شود. بنابراین، معلمان باید با دانش‌آموزان معاشرت کنند، بنابراین تمایل یا آمادگی برای یادگیری آن دارند. برای اطمینان از اینکه دانشجو تمایل و آمادگی برای یادگیری در مورد امنیت سایبری دارد، برنامه مطالعه باید یک برنامه یادگیری تعاملی و جالب باشد. برخی از دانش استانداردی که باید به دانش‌آموزان آموزش داده شود، در مورد کوکی‌های اینترنتی، فیشینگ وب و استفاده از وب‌سایت‌های تجارت الکترونیک است. کوکی های اینترنتی یکی از جدیدترین فناوری های جدید در زمینه مسائل وب سایت هستند. کوکی ها اعلانی است که همیشه در هنگام دسترسی کاربر به وب سایت به صورت اعلان روی صفحه رایانه یا صفحه تلفن همراه نشان داده می شود. اکثر کاربران معنی و هدف کوکی ها را درک نمی کنند. اخطار را نادیده می‌گیرند یا مستقیماً بدون اطلاع از مفهوم و پیشنهاد، اجازه یا رد می‌دهند. کوکی های اینترنتی قابلیتی هستند که به طور خودکار داده ها را در یک وب سایت ضبط یا بازیابی می کند. بنابراین داده های کاربران مانند نام آدرس ایمیل را می توان به خوبی در وب سایت ذخیره کرد [۱۵].

کوکی های اینترنتی که در مرورگر دیده می شوند به عنوان کوکی ساده، کوکی اینترنتی، کوکی وب یا کوکی نامگذاری می شوند. کوکی اینترنتی یک قطعه داده کوچک است که در نتیجه فعالیت های قبلی کاربر در وب سایت های خاص در رایانه ذخیره می شود [۲۶]. هدف از این داده های دیجیتالی به منظور ایجاد راحتی و سهولت در دسترسی به یک وب سایت، مانند تجارت الکترونیک است. برخی از مزایای استفاده از کوکی، نام کاربری و رمز عبور است که به طور خودکار توسط فناوری کوکی

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

ذخیره می شود. علاوه بر این، نام، آدرس و شماره کارت اعتباری که قبلاً در وب‌سایت‌ها وارد شده‌اند ذخیره شده و قابل دسترسی هستند.

علل ایجاد آسیب های دنیای مجازی برای دانش آموزان

الف) اکثر دانش آموزان از اهمیت بیان اطلاعات فردی نگران نیستند و به این ترتیب در معرض خطر تهاجمات بیش از حد وحی و امنیتی قرار دارند.اطلاعات فری خود را بر اساس اعتمادی که به دوستان خود دارند در دسترس آنان قرار می دهند و سپس سایر مهاجمان از آن اطلاعات علیه دانش آموز استفاده میکنند . به همین خاطر باید در مدارس به دانش آموزان آموخته شود که اطلاعات فردی جز حریم خصوصی فرد هست و نباید آنها را در دسترس افراد دیگر قرار بدهد [۱۵].

ب) دانش آموزانی که از آسیب ها آگاه هستند، به طرز تکان دهنده ای تنظیمات حفاظتی نامناسب را انتخاب می کنند و به طور مناسب بر تمایلات امنیتی نظارت می کنند. بدین منظور دانش آموزان مطلع از سواستفاده های مجازی از پسود ها و گذواژه ها و سیستم های امنیتی قوی برای حفظ اطلاعات خود استفاده می کنند و در هربازه زمانی مناسب آنها را تعویض می کنند تا از هک شدن احتمالی اطلاعات خود جلوگیری نمایند. رمزهای عبور ضعیف همچنان بزرگترین تهدید برای حریم خصوصی افراد هستند. مردم هنوز تمایل دارند به رمزهای عبور ضعیفی اعتماد کنند که به راحتی می توانند شکسته شوند و منجر به سرقت داده ها و آسیب پذیری های دیگر برای کاربر شود [۱۵]. این واحد شامل سه تمرین در مورد رمزهای عبور است:

این تمرین ابتدا به کاربر توضیح می دهد که چه چیزی یک رمز عبور خوب را ایجاد می کند. سپس از کاربر می خواهد که رمز عبور احتمالی را وارد کند. آن را تحلیل می کند؛ و جدولی را به کاربر ارائه می دهد که اطلاعاتی در مورد اجزای یک رمز عبور قوی دارد و چه مواردی را از دست داده است و همچنین تخمینی از اینکه چقدر طول می کشد تا رمز عبور بسته به مجموعه کاراکترهای استفاده شده در آن شکسته شود.

ب شکستن رمز عبور: در ادامه تمرین اول، این تمرین به طور مختصر نحوه عملکرد حملات دیکشنری را شرح می دهد و به کاربر اجازه می دهد تا رمز عبور (متشکل از حداکثر ۵ حرف کوچک برای صرف زمان) وارد کند و زمان بندی آن را ارائه می دهد. چه مدت طول می کشد تا رمز عبور با استفاده از یکی از روش ها شکسته شود.

ج گذرواژه‌های پیش‌فرض: پس از توضیح اینکه برخی از دستگاه‌ها دارای رمز عبور پیش‌فرض برای راه‌اندازی و دسترسی آسان هستند، این تمرین ویدئویی از یک کلیپ خبری را در اختیار کاربر قرار می‌دهد که در مورد استفاده از رمز عبور پیش‌فرض در وب‌کم هشدار می‌دهد. این تمرین همچنین پیوندی به وب سایتی ارائه می دهد که رمزهای عبور پیش فرض را برای بسیاری از دستگاه ها از جمله وب کم و روتر فهرست می کند.

چ) رویکرد و عملکرد به اندازه کافی برای مدیریت گستره وسیعی از آسیب های شبکه های اجتماعی که با مشکلات بیشتر، پیشرفت های امروزی و مدرن، گام به گام افزایش می یابد، تجهیز نشده است. بر همین اساس در مدارس باید رویکردهای لازم جهت مدیریت گستره آسیب های شبکه های اجتماعی اتخاذ گردد.

د) فقدان ابزار و سیستم احراز هویت مناسب برای مقابله و مدیریت مسائل مختلف امنیتی و حفاظتی. مدارس زمانی که سایت های لازم برای کسب اطلاعات را به دانش آموزان معرفی می کنند این سایت ها در اکثر مواقع از سیستم های احراز هویت در

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

برابر مسائل امنیتی برخوردار نیستند و به همین خاطر زمانی که دانش آموزی احراز هویت می کنند در دام تهدیدات و آسیب ها می افتند. امنیت مرورگر

برای بسیاری از مرورگرهای اینترنت پنجره هایی هستند که آنها را به دنیای سایبری متصل می کنند. مردم بیشتر فعالیت های خود را در اینترنت از طریق مرورگرهای وب انجام می دهند، اما کنترل مرورگر خود را به دست نمی گیرند. آنها اغلب تنظیمات پیش فرض را می پذیرند و نمی دانند که می توانند این تنظیمات را تغییر دهند.

راهکارهای پیشگری از آسیب های دنیای مجازی برای دانش آموزان

الف) ایجاد آگاهی در مورد افشای اطلاعات: - بیشتر دانش آمزوان در مورد افشای اطلاعات خود در پروفایل های سایت های اجتماعی به خوبی و به طور استثنایی آگاه نیستند برهمین اساس باید در طی جلسه های آموزشی دانش آموزان را از اهمیت و معایب افشای اطلاعات خود در هر سایتی آگاه ساخت [۱۵].

ب) تشویق آگاهی و نبردهای آموزند دولت ها باید در مورد مسائل آگاهی - افزایش و امنیت کلاس های آموزشی بدهند و ارائه دهند. تا زمانی که آموزش های کافی برای دانش آموزان وجود نداشته باشد آگاهی آنان افزایش نخواهد یافت.

ج) اصلاح قانون موجود: مصوبات موجود باید با نوآوری جدید و جعلیات و حملات جدید شناسایی شود. باید از وجود سایت های ناآشنا آگاهی یافت و به دانش آموزان در خصوص آسیب رسانی های آنان اطلاع رسانی کرد.

د) توانمندسازی احراز هویت: کنترل و احراز هویت باید به طور استثنایی محکم باشد تا جرایم سایبری انجام شده توسط برنامه نویسان، ارسال کنندگان هرزنامه و سایر مجرمان سایبری به هر میزان که به طور منطقی قابل انتظار باشد، کاهش یابد [۵].

ه) استفاده از قوی ترین ابزارهای آنتی ویروس: دانش آموزان باید از قوی ترین ابزارهای آنتی ویروس با به روز رسانی های معمولی استفاده کنند و باید تنظیمات پیش فرض مناسب را حفظ کنند تا ابزارهای آنتی ویروس با موفقیت بیشتری کار کنند.و در این صورت تا حدودی رایانه های شخصی آنان از حملات ناگهانی مهاجمان در امان خواهد بود. و دانش آموزان با خیالی آسوده می توانند به سایت های اطلاعاتی مراجعه نمایند.

و) ارائه ابزارهای امنیتی مناسب : مدارس باید ابزارهای منحصر به فردی را برای دانش آموزان ارائه دهند که آنها را قادر می سازد تا سوابق خود را تخلیه کنند و بر مسائل حریم خصوصی و امنیتی متمایز نظارت و کنترل کنند. از جمله ابزارهای امنیتی مناسب استفاده از نرم افزارهای مناسب و کنترل شده مثل نرم افزار شاد استفاده می کنند.

ح) نیاز به تغییرات بیشتر برای شبکه های اجتماعی با این هدف که بتوانند دانش آموزان را قادر سازند تا با پروفایل ها و ابزارهای ارتباطی خود برخورد کنند[۱۶].

خ) لازمه عضویت و ادغام شبکه های اجتماعی و جهان های مجازی آینده را برای دانش آموزان آموزش بدهند.

ذ) نیاز به یکپارچه سازی اطلاعات از شبکه های مختلف، به عنوان مثال اثبات قابل تشخیص همه مواد شناسایی شده با موضوع خاص. این نیاز به دستورالعمل‌های خاص و نوآوری اصلاح‌شده توسط تامین‌کنندگان شبکه‌های اجتماعی دارد.

ر) بسیاری از شبکه های اجتماعی به رابط های برنامه نویسی برنامه کاربردی استاندارد نیاز دارند، بنابراین دانش آموزان می توانند اطلاعات پروفایل خود را با استفاده از ابزارهای استاندارد وارد کرده و دریافت کنند.به عنوان مثال، فیس بوک و گوگل

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

نوآوری های جدیدی را به هم متصل کرده اند که امکان تطبیق پذیری اطلاعات دانش آموزان را در میان سایت های اجتماعی فراهم می کند، که نشان دهنده یک منبع رقابت دیگر در بین مدیریت شبکه های اجتماعی است

پیشرفت‌ها در سایت‌های اجتماعی و استفاده از تلفن همراه با افزودن نکات برجسته و برنامه‌های کاربردی بیشتر به تلفن‌های همراه و همچنین تلویزیون‌های اجتماعی برای گفتگو، ایمیل، و ویدئو کنفرانس ،گردهمایی‌های آینده، بر رشد استفاده از شبکه‌های اجتماعی قابل حمل تأثیر می‌گذارد. [۱۷].

علل انزوای اجتماعی دانش‌آموزان

علل واقعی انزوای اجتماعی در دانش‌آموزان می‌تواند به انواع مختلفی باز شود و از جوانب مختلف زندگی شخصی و تحصیلی آنان ناشی شود. در زیر به برخی از علل اصلی انزوای اجتماعی در دانش‌آموزان اشاره می‌شود:

۱. عدم انطباق اجتماعی:

دانش‌آموزان ممکن است با مشکلات انطباق اجتماعی مواجه شوند که باعث ایجاد فاصله و انزوای اجتماعی شود. این مشکلات می‌توانند ناشی از اختلافات فرهنگی، اجتماعی یا رفتاری باشند.

۲. ضعف مهارت‌های ارتباطی:

دانش‌آموزانی که مهارت‌های ارتباطی قوی ندارند، ممکن است در برقراری ارتباطات دوستانه و اجتماعی مشکل داشته باشند و احساس انزوای اجتماعی نمایند [۱۷].

۳. تفاوت‌های شخصیتی:

تفاوت‌های شخصیتی و علایق ممکن است باعث ایجاد انزوای اجتماعی شود، زیرا فرد ممکن است احساس کند که نمی‌تواند با دیگران درک و هماهنگ شود.

۴. مشکلات خانوادگی:

مشکلات در خانواده، مثل طلاق و یا مشکلات مالی، ممکن است تأثیرات منفی بر روحیه دانش‌آموز داشته باشد و او را به انزوای اجتماعی بکشاند.

۵. عدم اطمینان از خود:

دانش‌آموزانی که از خود اطمینان کمی دارند، ممکن است احساس کنند که نمی‌توانند به گروهی متعلق شوند و این امر باعث انزوای اجتماعی آنان شود.

۶. تغییرات محیطی:

تغییر محیط زندگی، مثل انتقال به یک مدرسه جدید یا شهری دیگر، می‌تواند باعث ایجاد انزوای اجتماعی در دانش‌آموزان شود.

۷. تجربه سوء در ارتباطات گذشته:

تجربه تعارضات یا ناکامی‌های قبلی در ارتباطات اجتماعی ممکن است باعث ترس از برقراری ارتباطات جدید شود.

۸. نبود فعالیت‌های گروهی:

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

فعالیت‌های گروهی و همکاری با دیگران، اغلب یک راه برای کاهش انزوای اجتماعی و ایجاد ارتباطات مثبت است. در صورتی که دانش‌آموزان در فعالیت‌های گروهی شرکت نکنند، احتمال تجربه انزوای اجتماعی بیشتر می‌شود[۱۹].

۹. فشارهای اجتماعی:

فشارهای اجتماعی ممکن است دانش‌آموزان را به انزوای اجتماعی و انزوا بکشاند، زیرا احساس می‌کنند که نمی‌توانند با استانداردها و انتظارات اجتماعی هماهنگ شوند.

۱۰. تأثیرات منفی شبکه‌های اجتماعی:

هرچند شبکه‌های اجتماعی ابزاری قدرتمند برای ارتباط است، اما ممکن است تأثیرات منفی هم داشته باشند؛ به عنوان مثال، مقایسه خود با دیگران، تحریک‌های منفی و افزایش احساس انزوای اجتماعی.

۱۱. ضعف مهارت‌های اجتماعی:

ضعف در مهارت‌های اجتماعی می‌تواند باعث شود دانش‌آموزان در مواقع ارتباطی دچار اضطراب شوند و از برقراری ارتباطات به خوبی منع شوند.

۱۲. عدم دسترسی به فرصت‌های اجتماعی:

برخی دانش‌آموزان ممکن است به علت شرایط خاص، محدودیت‌های مکانی یا اجتماعی، به فرصت‌های کافی برای برقراری ارتباطات اجتماعی دسترسی نداشته باشند [۱۸].

با توجه به این موارد، می‌توان با ارائه راهکارهایی مناسب و ارتقاء مهارت‌های اجتماعی، به دانش‌آموزان کمک کرد تا از انزوای اجتماعی خود آگاه شوند و بهبودی در ارتباطات اجتماعی خود حاصل کنند.

راهکارهای مقابله با انزوای اجتماعی در شبکه‌های اجتماعی

راهکارهایی برای کاهش انزوای اجتماعی دانش‌آموزان در شبکه‌های اجتماعی:

۱. تشویق به مشارکت فعال:

تشویق دانش‌آموزان به مشارکت فعال در گروه‌ها و فعالیت‌های آموزشی آنلاین می‌تواند ارتباطات آنان را تقویت کرده و احساس تعلق به یک جامعه آنلاین را بالا ببرد.

۲. آگاهی از رفتارهای اجتماعی:

افزایش آگاهی دانش‌آموزان از رفتارهای اجتماعی مثبت و احترام به دیگران، می‌تواند به ایجاد محیطی دوستانه‌تر و حاکم بر احترام متقابل در شبکه‌های اجتماعی کمک کند.

۳. ترویج فعالیت‌های گروهی و همکاری:

ارتقاء فعالیت‌های گروهی و همکاری در پروژه‌ها و تکالیف می‌تواند افراد را به تعامل بیشتر و اشتراک گذاری تجربیات و دانش وادار کند.

۴. ساخت دنیای مجازی حمایت‌آمیز:

ایجاد یک دنیای مجازی حمایت‌آمیز و دوستانه در شبکه‌های اجتماعی، با فراهم کردن فرصت‌های مثبت برای ارتباط و اشتراک گذاری، می‌تواند احساس انزوای اجتماعی را کاهش دهد [۱۱].

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

۵. آموزش مهارت‌های ارتباطی:

آموزش مهارت‌های ارتباطی به دانش‌آموزان، از جمله گوش دادن فعال، ارتباط برقرار کردن و حل اختلافات، می‌تواند بهبود در ارتباطات شبکه‌های اجتماعی آنان ایجاد کند.

۶. رصد و پیگیری انزوای اجتماعی:

ارائه ابزارها و منابعی برای رصد و پیگیری احساس انزوای اجتماعی در دانش‌آموزان، به مدیران و مربیان کمک می‌کند تا به سرعت واکنش نشان دهند و راهنمایی لازم را ارائه کنند.

۷. ترویج فعالیت‌های اجتماعی متنوع:

تشویق دانش‌آموزان به شرکت در فعالیت‌های اجتماعی متنوع، از جمله گروه‌های علمی، هنری یا ورزشی، می‌تواند آنان را به ارتباط با همدیگر بیشتر کند و از ایجاد انزوای اجتماعی جلوگیری نماید.

۸. ارتقاء افکار مثبت و خودارزیابی:

تربیت افکار مثبت و تشویق به خودارزیابی می‌تواند از دانش‌آموزان در مواجهه با چالش‌ها و احساس انزوای اجتماعی، استفاده اثربخشی داشته باشد. افراز نگرش‌های سازنده و افزایش اعتماد به نفس، ارتقای ارتباطات اجتماعی را تسهیل می‌کند.

۹. استفاده مثبت از فناوری:

اطلاعیه‌ها، وبلاگ‌ها و پلتفرم‌های آموزشی را به گونه‌ای به‌کار ببرید که ارتباطات مثبت را ترویج کنند و به دانش‌آموزان اجازه دهند تا تجربیات و دانش خود را به اشتراک بگذارند.

۱۰. تشکیل جلسات تحت نظر:

برگزاری جلسات تحت نظر با موضوعات مرتبط با ارتباطات اجتماعی و راهکارهای مقابله با انزوای اجتماعی، فرصت مناسبی برای آموزش و تبادل نظر فراهم می‌کند. این جلسات می‌توانند ارتباطات دانش‌آموزان را تقویت کرده و آنان را به اشتراک‌گذاری تجربیات و مشکلات بیشتر ترغیب کنند.

۱۱. ترویج همکاری با والدین:

همکاری فعال با والدین به منظور تربیت کودکان به عنوان اعضای فعال در شبکه‌های اجتماعی و تشویق آنان به شرکت در فعالیت‌های گروهی، می‌تواند از انزوای اجتماعی دانش‌آموزان جلوگیری نماید.

۱۲. ارائه منابع حمایتی:

ارائه منابع آموزشی و مشاوره‌ای در زمینه‌های ارتباطات اجتماعی و رفع احساس انزوای اجتماعی، به دانش‌آموزان کمک می‌کند تا بهترین راه‌حل‌ها را برای مواجهه با چالش‌های اجتماعی پیدا کنند [۱۲].

با توجه به اهمیت ارتباطات اجتماعی در رشد و توسعه دانش‌آموزان، اجرای این راهکارها می‌تواند بهبود قابل توجهی در ایجاد یک جامعه دوستانه و حمایتی در شبکه‌های اجتماعی داشته باشد.

نتیجه گیری

در برخورد با چالش انزوای اجتماعی در دانش‌آموزان، مهمترین گام تحلیل علل و اندازه‌گیری اثرات آن است. با توجه به عوامل متعددی که می‌تواند انزوای اجتماعی را در این گروه ایجاد کند، ایجاد راهکارهای گسترده و شامل اساسی است. اهمیت

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

ارتباطات اجتماعی در توسعه روانی و تحصیلی دانش‌آموزان ناگزیر کرده است که به مسائل انزوای اجتماعی با دقت و توجه پرداخته شود. توازن میان تشویق به فعالیت‌های گروهی، ارتقاء مهارت‌های ارتباطی، و مدیریت فشارهای اجتماعی، می‌تواند بهبود محیط اجتماعی دانش‌آموزان را به همراه داشته باشد.

اگرچه سایت‌های شبکه‌های اجتماعی فناوری تعامل و ارتباطات را ارائه می‌دهند، اما مشکلات جدیدی را در مورد مسائل مربوط به حریم خصوصی و امنیتی ایجاد می‌کنند. پیشرفت فناوری جدید به عنوان یک قاعده و سایت های اجتماعی به طور خاص خطرات امنیتی جدیدی را به همراه خواهد داشت که ممکن است درهای باز را برای هنرمندان نمایش انتقام جو، چوب بران کلیدی، اسب های تروا، فیشینگ، جاسوسان، ویروس ها و مهاجمان باز کند. متخصصان امنیت اطلاعات، مقامات دولتی و سایر افسران اطلاعاتی باید ابزارهای جدیدی را توسعه دهند که با خطرات و تهدیدهای احتمالی آینده مقابله کرده و با آنها سازگار شوند. همچنین می تواند به طور ایمن میزان عظیم اطلاعات را در اینترنت و سایت های اجتماعی نیز کنترل کند. برای پیشگیری از آسیب های دنیای مجازی پیشنهاد ضروری برای فعال کردن شبکه‌های سیستم اجتماعی برای دانش آموزان ذکر کرده اند که عبارتند از:

الف) همیشه در پیام های خود و سایر سایت های اجتماعی گذرواژه های بسیار قوی داشته باشید.

ب) محدود کردن اطلاعات شخصی در سایت های اجتماعی تا آنجا که می توانید.

پ) رمزهای عبور خود را به طور مداوم تغییر دهید، با این هدف که اطلاعات شما توسط برنامه نویسان از راه دور باشد.

ت) به دلیل شهرت اینترنت، حداقل اطلاعات را در اختیار سایت و اینترنت قرار دهید.

ث) به دیگران آنلاین اعتماد نکنید و به سؤالات غیر معمول مشتریان یا سازمان‌های مبهم پاسخ ندهید، یعنی مراقب باشید.

ج) سیاست های حفظ حریم خصوصی را بررسی کنید و از پیام ها و پیوندهای مبهم ارائه شده توسط دانش آموزان مبهم مطلع شوید.

در این مقاله، به تحلیل علل و ارائه راهکارهایی برای کاهش انزوای اجتماعی دانش‌آموزان در شبکه‌های اجتماعی پرداختیم. با شناخت بهتر از علل این احساس ناخوشایند، می‌توانیم به شکل‌گیری راهکارهای کارآمدتر و مؤثرتر کمک کنیم. استفاده از روش‌های آموزشی و تربیتی، ترویج فعالیت‌های گروهی، ارتقاء مهارت‌های اجتماعی و توجه به جوانب روانی دانش‌آموزان، می‌تواند به ساختارهای اجتماعی دوستانه و حامی در شبکه‌های اجتماعی منجر شود. این اقدامات نه‌تنها بر تجربه تحصیلی دانش‌آموزان مؤثر خواهد بود بلکه به ساخت یک جامعه مدرسه فعال و پویا نیز کمک خواهد کرد.

ISSN ۲۹۸۰-۷۷۸۶

منابع

1. Baraković, S., & Baraković Husić, J. (202۰). Cyber hygiene knowledge, awareness, and behavioral practices of university students. Information Security Journal: A Global Perspective, 1-24.
2. Btoush, M., Alarabeyat, A., ZBOON, M., RYATI, O., HASSAN, M., & AHMAD, S. (2011). INCREASING INFORMATION SECURITY INSIDE ORGANIZATIONS THROUGH AWARENESS LEARNING FOR EMPLOYEES. Journal of Theoretical & Applied Information Technology, 24(2).
3. Desai, N., Pathari, K., Raut, J., & Solavande, V. (2018). Online surveillance for exam. Jung, 4(03).
4. Ip, W. H. (2013). Am I being watched on the internet?: examining user perceptions of privacy, stress and self-monitoring under online surveillance.
5. Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. ACM Transactions on Computing Education (TOCE), 18(3), 1-12.
6. Kritzinger, E., Bada, M., & Nurse, J. R. (2017, May). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In IFIP World Conference on Information Security Education (pp. 110-120). Springer, Cham.
7. McIntyre, A. (2018). Developing a Cybersecurity Protocol for Your Operational Environment. Natural gas & electricity, 34(9), 23-27.
8. Paul, P., Biswas, B. A., Khalid, Z., Biswas, S., Dutta, N., Saha, H. N., & Das, M. (2018, November). Using Browser Cookies for Event Monitoring and User Verification of an Account. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 455-460). IEEE.
9. Persadha, P. D., Waskita, A. A., Fadhila, M. I., Kamal, A., & Yazid, S. (2016, January). How inter-organizational knowledge sharing drives national cyber security awareness?: A case study in Indonesia. In 2016 18th International Conference on Advanced Communication Technology (ICACT) (pp. 550-555). IEEE
10. Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. Journal of Digital Learning in Teacher Education, 28(2), 82-85.
11. Sekyere, B. O. (2015). Studying Information Security Behaviour among Students in Tertiary Institutions.
12. Shahin, E. (2017). Is Wifi Worth It: The Hidden Dangers Of Public Wifi. Catholic University Journal of Law and Technology, 25(1), 7.
13. Susser, D. (2019). Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't. Journal of Information Policy, 9(1), 148-173.
14. Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Hallatu, T. G. R. (2019). Cybercrime case as impact development of communication technology that troubling society. Int. J. Sci. Technol. Res, 8(9), 1224-1228.
15. Z. Tayibnapis, L. E. Wuryaningsih, and R. Gora, "The Development of Digital Economy in Indonesia," IJMBS International Journal of Management and Business Studies, vol. 8, no. 3, pp. 1418, 2018.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

۱۶. رحمانی, & ایل بیگی. (۱۴۰۰). نقش ابعاد شخصیتی هگزاکو و نگرش‌های مذهبی و هوش اخلاقی در پیش‌بینی آسیب‌های فضای مجازی در دانش‌آموزان دختر دوره دوم مقطع متوسطه شهر مشهد. *نشریه علمی رویش روان شناسی*, *۱۰*(۱۱), ۲۱۹-۲۲۸.

۱۷. رسولی.(۱۴۰۰). تحلیل عصبی شناختی آسیب های رسانه ها نوین اجتماعی. مطالعات بین رشته ای در رسانه و فرهنگ/۱۱(۲).

۱۸. کاظمی آرپناهی، مهری،(۱۴۰۱)،شناسایی مشکل انزوا و گوشه گیری دانش آموز و راهکارهای بهبود آن،بیست و چهارمین کنفرانس بین المللی پژوهش های نوین در علوم و فناوری،کرمان

۱۹. محمدی، صدیقه و رامش، امیر رضا،(۱۳۹۸)،بررسی اثر بخشی درمان شناختی رفتاری گروهی بر کاهش اعتیاد به اینترنت و احساس تنهایی و بهبود عملکرد تحصیلی در پسران دانش آموز دبیرستانی،پنجمین کنفرانس ملی نوآوری های اخیر در روانشناسی،کاربردها و توانمندسازی با محوریت رواندرمانی،تهران.