Applied Criminology Research
پژوهش های جرم شناسی کاربردی
دوره ۲ / شماره ۵/ پاییز ۱۴۰۳
تاریخ دریافت: ۱۴۰۳/۰۳/۱۱
تاریخ پذیرش: ۱۴۰۳/۰۶/۲۸
صفحه: ۷۳ الی ۱۰۰
Volume 2, Issue 5, Autumn 2024
Received: 2024/05/31
Accepted: 2024/09/18
Pages: 73-100
Article Type: **Research**
نوع مقاله: پژوهشی
System: qacr.ir doi: 10.22034/AQCR.2025.2049961.1048

The role of education in preventing cyber victimization

Mireltefat Ale Rasool Komarolia✉[1], Massuod Morshedy[2]

Abstract

Field and Aims: Common forms of cybercrimes, which include the exploitation of the human element through social engineering methods, have grown significantly with the use of technology and internet services in most areas of human life and have become a global threat. Since the success rate and damage of these cyber attacks are very high, organizations and individuals should be adequately informed about how to prevent these attacks. Therefore, education becomes important as a cornerstone of learning in cybercrime prevention programs. In this regard, the present research was conducted with the aim of explaining the roles that education can play in preventing cyber victimization.

Method: In terms of purpose, application and data collection, the present research was conducted using a library method.

Findings and Conclusions: Cyber security and crime prevention training programs with "creating fundamental knowledge", "raising the level of public digital literacy", "increasing responsible online behavior", "developing critical thinking skills", "filling the knowledge gap", "strengthening Parental monitoring", "increasing social participation", "training of expert manpower", "victim empowerment" can play a very important role in preventing cybercrimes.

Cyber security training and responsible digital citizen training can directly and indirectly affect users' security behaviors and increase their level of knowledge and motivation to implement preventive measures. Improving public awareness of cybercrimes through digital literacy training under targeted educational programs can be significantly effective in preventing cybercrimes.

Keyword: cyber security education, digital knowledge, cyber literacy, prevention.

❋Citation (APA): Ale Rasool Komarolia, M.; Morshedy, M. (2024). The role of education in preventing cyber victimization. *Applied criminology research*, 2(5), 73-100. https://www.qacr.ir/article_722325.html

1. Master of Criminal Law and Criminology University of Shahid Beheshti, Tehran, Iran. Email: massuodmorshedy@yahoo.com
2. Assistant Professor of Criminal Investigation, Amin University of Police Sciences, Tehran, Iran. Email: massuodmorshedy@yahoo.com

دوره ۲ / شماره ۵/ پاییز ۱۴۰۳
تاریخ دریافت: ۱۴۰۳/۰۳/۱۱
تاریخ پذیرش: ۱۴۰۳/۰۶/۲۸
صفحه: ۷۳ الی ۱۰۰

پژوهش های جرم شناسی کاربردی
Applied Criminology Research

Volume 2, Issue 5, Autumn 2024
Received: 2024/05/31
Accepted: 2024/09/18
Pages: 73-100

نوع مقاله: پژوهشی
Article Type: **Research**

doi: 10.22034/AQCR.2025.2049961.1048
سامانه: qacr.ir

نقش آموزش در پیشگیری از بزه‌دیدگی سایبری

میرالتفات آل رسول کمارعلیا✉[۱]، مسعود مرشدی[۲]

چکیده

زمینه و هدف: اشکال رایج جرائم سایبری که شامل بهره‌گیری از عنصر انسانی از طریق روش‌های مهندسی اجتماعی می‌شود، با کاربست فناوری و خدمات اینترنتی در اکثر ساحت زندگی بشری، رشد چشمگیری داشته و به یک تهدید در سطح جهانی بدل گشته است. از آنجایی که نرخ موفقیت و خسارت این حملات سایبری بسیار بالا است، سازمان‌ها و افراد باید به اندازه کافی در مورد چگونگی پیشگیری از این حملات مطلع شوند. بنابراین، آموزش به عنوان سنگ‌بنای یادگیری در برنامه‌های پیشگیری از جرائم سایبری اهمیت پیدا می‌کند. در این راستا، پژوهش حاضر با هدف تبیین نقش‌هایی که آموزش می‌تواند در پیشگیری از بزه‌دیدگی سایبری ایفا نماید، صورت پذیرفت.

روش: پژوهش حاضر از نظر هدف، کاربردی و به لحاظ گردآوری داده، به روش کتابخانه‌ای انجام شده است.

یافته‌ها و نتایج: برنامه‌های آموزش امنیت سایبری و پیشگیری از جرم با «ایجاد دانش بنیادی»، «بالابردن سطح سواد دیجیتال عمومی»، «افزایش رفتار مسئولانه آنلاین»، «توسعه مهارت‌های تفکر انتقادی»، «پرکردن شکاف دانش»، «تقویت نظارت والدین»، «افزایش مشارکت اجتماعی»، «تربیت نیروی انسانی متخصص»، «توانمندسازی قربانیان»، نقش بسیار مهمی را می‌تواند در پیشگیری از جرائم سایبری ایفا کند.

آموزش امنیت سایبری و تربیت شهروند دیجیتال مسئول می‌تواند به طور مستقیم و غیرمستقیم، رفتارهای امنیتی کاربران را تحت تأثیر قرار دهد و سطح دانش و انگیزه‌های آنها را برای اجرای تدابیر پیشگیرانه افزایش دهد. ارتقای آگاهی عمومی نسبت به جرائم سایبری از طریق آموزش سواد دیجیتالی تحت برنامه‌های آموزشی هدفمند می‌تواند به صورت چشمگیری در پیشگیری از جرائم سایبری مؤثر باشد.

کلیدواژه‌ها: آموزش امنیت سایبری، دانش دیجیتال، سواد سایبری، پیشگیری.

استناددهی (APA): آل رسول کمارعلیا، میرالتفات؛ مرشدی، مسعود. (۱۴۰۳). نقش آموزش در پیشگیری از بزه‌دیدگی سایبری. *پژوهش‌های جرم‌شناسی کاربردی*، ۲(۵)، ۱۰۰-۷۳.

https://www.qacr.ir/article_722325.html

---

۱. کارشناسی‌ارشد حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی، تهران، ایران.
رایانامه: aalerasoulmireltefat@gmail.com

۲. استادیار جرم یابی دانشگاه علوم انتظامی امین، تهران، ایران. رایانامه: massuodmorshedy@yahoo.com

مقدمه

گسترش روزافزون فناوری‌های اطلاعات و ارتباطات، ظهور شبکه جهانی وب، تلفن‌های هوشمند و ورود آنها به زندگی بشر، دریچه‌ای نوین را به روی انسان معاصر گشوده و همه جنبه‌های زندگی بشر را دگرگون ساخته است. افراد به طور فزاینده‌ای برای نیازهای روزمره، از تجارت گرفته تا تعاملات اجتماعی، به فناوری تکیه می‌کنند. برای اکثر مردم جهان، فناوری به بخشی جدایی‌ناپذیر از زندگی روزمره تبدیل شده است (هولت و بوسلر[1]، ۲۰۱٤: ۲۱). بر اساس آمار در سال ۲۰۱۹، حدود ٤,٤٨ میلیارد کاربر اینترنت در سراسر جهان با ضریب نفوذ ۵۷ درصد در میان جمعیت جهان وجود داشت (درو[2]، ۲۰۲۰: ۱۷). در این میان، با شروع محدودیت‌های کووید ۱۹ در سراسر جهان به‌ویژه ایران، استفاده از خدمات اینترنتی ٤۰ تا ۱۰۰ درصد در مقایسه با سطوح پیش از قرنطینه افزایش یافت (دی[3] و همکاران، ۲۰۲۰: ۱؛ صادقی، ۱۳۹۹)؛ و به ادغام سریع فضاهای فیزیکی و سایبری و افزایش اتکا به اتصال برای بسیاری از کارهای اساسی، هم در زندگی کاری و هم در زندگی شخصی سرعت بخشید؛ بطوری که شمار کاربران اینترنت به ۵,۳ میلیارد کاربر در سال ۲۰۲۳ رسیده است که ٦۵,۷ درصد از جمعیت جهان را تشکیل می‌دهد (استاتیسکا[4]، ۲۰۲۳؛ آل رسول، ۱٤۰۱: ۳). همزمان با جهانی‌شدن ارتباطات و اطلاعات و نهادینه‌شدن بیشتر فناوری اطلاعات در جوامع، بخش تاریکی نیز در کنار تمام فواید، محسنات و توانایی‌های غیرقابل‌تصور فضای سایبری شکل گرفته است (درویشی و همکاران، ۱٤۰۳: ۳۵؛ جایشانکار[5]، ۱۳۹۵: ۱۵۵) و با بهره‌گیری از ویژگی‌های انحصاری این فضا همچون سرعت، قابلیت گمنامی، فرامکانی‌بودن، سیالیت، خودکاربودن و غیره، رشد و توسعه یافت. این بخش تاریک که از آن با عنوان جرائم سایبری یاد می‌شود، یک بازار و اقتصاد غیرقانونی چندتریلیون دلاری در جهان را شکل داده (مورگان[6]، ۲۰۲۰) و به یک خطر و تهدید عمومی در مقیاس جهانی تبدیل شده است. افراد با انگیزه‌های مجرمانه خود را با ابزارها و فناوری‌های جدید به خوبی سازگار کرده و فعالیت‌های غیرقانونی خود را از فضای واقعی به فضای مجازی منتقل کرده و از این طریق نه تنها بخش دولتی، بلکه بخش خصوصی و حتی افراد عادی را نیز مورد هدف قرار می‌دهند؛ همچنین، از این طریق،

1. Holt & Bossler
2. Drew
3. De et al
4. Statista
5. Jaishankar
6. Morgan

چالش‌های جدی را برای تمام ساحت‌های زیست مجازی ازجمله تجارت و بانکداری الکترونیک، ایجاد می‌کنند.

امنیت مهم‌ترین رکن پایداری یک جامعه است و مبارزه با جرائم حوزه سایبری نیز یکی از ارکان مهم امنیت سایبری محسوب می‌گردد (صبح خیز، پورقهرمانی و صفاری، ۱۳۹۹: ۱۰۹). تأمین امنیت شهروندان و پیشگیری از بزه‌دیده واقع‌شدن آنان در فضای سایبری نیز همانند دنیای حقیقی از وظایف ذاتی دولت‌هاست که امروزه، به چالش جدی برای آنان بدل گشته است؛ زیرا رویکردهای سنتی و سازمان‌های مجری قانون که وظیفه اصلی کنترل جرم را برعهده دارند، در پیشگیری از وقوع جرائم سایبری، شناسایی و دستگیری مجرمان سایبری در دنیای دیجیتال و به‌هم‌پیوسته فناوری که اکنون در آن زندگی می‌کنیم، به دلیل قابلیت ناشناس‌ماندن در اینترنت برای مجرمان، پراکندگی جغرافیایی بزه‌دیدگان، با بزهکارانی که معمولاً خارج از محدوده قضایی مجریان قانون محلی قرار دارند، با مشکلات چالش‌برانگیز متعددی روبه‌رو هستند؛ زیرا شیوه عمل مجرمان سایبری اغلب رویکردهای پلیسی سنتی را بی‌اثر می‌کند (هالدر[1]، ۲۰۲۲: ۵۲؛ عبدالله و جهان[2]، ۲۰۲: ۲۲٤؛ وبستر و درو[3]، ۲۰۱۷: ۳۹). از سوی دیگر، خلوت اینترنت و ماهیت فضای سایبری و وجود ابزارها و فناوری‌های نوین و روزآمدسازی و توسعه ثانیه‌شمار آنها و همچنین، قابلیت‌هایی چون امکان گمنامی کارآمدی سیاست‌های سلبی و محدودکننده مانند فیلترینگ، راهبردهای پیشگیری وضعی و اجتماعی از جرائم سایبری را با تردیدهای جدی مواجه ساخته است (جزایری و همکاران، ۱۳۹۸: ٤٦؛ جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱٤۹)؛ از سوی دیگر، کاربرانی که با تهدیدهای جدی و فراگیری مواجه هستند. با وجود گزارش‌های مکرر از تلفات ناشی از نقض امنیت رایانه، بسیاری از افراد هنوز اقدامات احتیاطی اولیه ایمنی را رعایت نمی‌کنند (جمیل[4]، ۲۰۲۲: ۱؛ شیلر[5] و همکاران، ۲۰۱۵: ۱۹۹). به بیان دیگر، اگر بهترین سیستم سخت‌افزاری یا سیستم عامل به کار گرفته شود، ولی کاربران یا عامل انسانی درگیر در یک سامانه رایانه‌ای، پارامترهای امنیتی را رعایت نکند، کاری را از پیش نخواهد برد (جامی پور، فرازپور و اسدی، ۱۳۹۹: ۱۰۹). به همین دلیل، اندیشمندان حوزه جرم‌شناسی و امنیت سایبری در مواجهه با اشکال جدید بزهکاری مرتبط با افزایش کاربران اینترنت، عامل انسانی را اغلب به عنوان ضعیف‌ترین

1. Halder
2. Abdullah & Jahan
3. Webster & Drew
4. Jamil
5. Shillair et al

حلقه در امنیت سایبری در نظر می‌گیرند (جوشی و دشپند[1]، ۲۰۲۲: ۹۷؛ جمیل، ۲۰۲۲: ۱۳۷؛ سریساوانگ[2] و همکاران، ۲۰۱۵: ۱۱؛ لوکفلد[3]، ۲۰۱۷: ۵۰). نتایج بسیاری از تحقیقات نشان می‌دهد که عدم رفتار ایمن کاربران و نقش آنان در بزه‌دیدگی سایبری ریشه در ضعف سواد سایبری و ناآگاهی آنان نسبت به تهدیدات نوظهور و نحوه رفتار صحیح در محیط مجازی دارد (ابراهیمی، صابری و لکی، ۱٤۰۱: ۵۳؛ محمودی، ۱٤۰۰: ۲۵؛ میر، ۱۳۹٤: ٦۰). به این ترتیب، بیش از پیش ضرورت و اهمیت اتخاذ راهبردهای آموزش‌محور، به‌عنوان راهکار منطقی و علمی ناظر به سیاست‌های پیشگیری اجتماعی در راستای افزایش خودایمن‌سازی در فضای مجازی، روشن می‌گردد (رضوی فرد، رباط جزی و عمرانی، ۱۳۹۷: ٦۳). در همین راستا، مقاله حاضر با هدف تبیین نقش‌هایی که آموزش می‌تواند در پیشگیری از بزه‌دیدگی سایبری ایفا نماید، انجام پذیرفت. لذا، پژوهش حاضر به دنبال پاسخ به این سؤال است که آموزش چه نقشی می‌تواند در پیشگیری از بزه‌دیدگی سایبری داشته باشد؟

1. Shriniwas Joshi &Pallavi Kulkarni Dshpand.
2. Srisawang et al
3. Leukfeldt

مبانی نظری و پیشینه تحقیق

پیشینه تحقیق

پژوهشگر	سال	عنوان	نتایج
جوشی و دشپند[1]	۲۰۲۲	آموزش جرائم سایبری	**۹۵ درصد حوادث امنیت سایبری شامل خطاهای انسانی است، بنابراین آموزش هوشمندانه‌ترین سرمایه‌گذاری در امنیت سایبری است. آموزش امنیت سایبری منجر به افزایش آگاهی از تهدیدات امنیتی و کاهش آسیب‌پذیری در افراد، خانواده‌ها، مشاغل، دولت‌ها و مؤسسات آموزشی شده و این امر به حذف خطاهای ناشی از مهندسی اجتماعی و سهل‌انگاری کمک می‌کند.**
جمیل	۲۰۲۱	عوامل مؤثر بر رویه‌های امنیت سایبری کاربران: مطالعه‌ای درباره کسب‌وکارهای خرد استرالیا	**متخصصان و کارشناسان امنیتی توصیه می‌کنند که نصب یک مدیررمز عبور برای ذخیره رمزهای عبور حیاتی است. با این حال، تحقیقات انجام‌شده برای این مطالعه نشان می‌دهد که چنین نرم‌افزاری دارای حداقل میزان استفاده است؛ علاوه بر این، تحقیقات کمی در مورد پذیرش آن وجود دارد. کاربرانی که تجربه و دانش بیشتری در زمینه امنیت سایبری دارند، به احتمال زیاد نرم‌افزارهای امنیتی را روی رایانه خود نصب می‌کنند.**
کورتیس و آکسبورگ[2]	۲۰۲۱	درک جرائم سایبری در «دنیای واقعی» پلیسی‌گری و اجرای قانون	**آموزش نیروها برای افزایش دانش و ارائه پاسخ‌های استاندارد به گزارش‌های جرائم سایبری و همچنین، افزایش مشارکت عمومی ممکن است به بهبود نرخ‌ها و تجارب گزارش‌دهی کمک کند. افزایش دانش در مورد جرائم سایبری و افراد درگیر می‌تواند با ایجاد آمادگی تحقیقاتی، توانایی همدلی با قربانیان را برای به‌دست‌آوردن نتایج بهتر در مصاحبه، تولید سرنخ‌های دقیق‌تر و شناسایی شواهد مناسب افزایش دهد.**
تدین، نادری و عزیزی کاکوندی	۲۰۲۱	نقش آموزش در پیشگیری از بزه‌دیدگی اطفال و نوجوانان در فضای مجازی	**افزایش دانش معلمان به فضای مجازی، تدوین دروس آموزشی جهت افزایش سواد فضای مجازی دانش‌آموزان در مدارس، افزایش نظارت و کنترل مدیران و معاونان مدارس، ایجاد همدلی میان دانش‌آموزان و معلمان در پیشگیری از بزه‌دیدگی مؤثر هستند.**

1. Shriniwas Joshi &Pallavi Kulkarni Dshpand
2. Joanna Curtis & Gavin Oxburgh

بروجنی، موذن و بهشتی	۱۴۰۲	پیشگیری غیرکیفری از بزه‌دیدگی زنان در فضای سایبری	**اطلاع‌رسانی عمومی از طریق رسانه‌های جمعی، آموزش و ارتقاء سواد سایبری، آموزش فرهنگ‌سازی استفاده صحیح از شبکه‌های مجازی از جمله راهکارهای پیشگیری اجتماعی از بزه‌دیدگی زنان در فضای سایبری است.**
ابراهیمی، صابری و لکی	۱۴۰۲	نقش سواد دیجیتال و خودمراقبتی در بزه‌دیدگی در فضای مجازی	**یافته‌های پژوهش نشان داد که بین سواد دیجیتال و خودمراقبتی در فضای مجازی و ابعاد بزه‌دیدگی در فضای مجازی رابطهٔ منفی و معنی‌دار وجود دارد. لذا، ضرورت آموزش در حوزهٔ خودمراقبتی در فضای مجازی و سواد دیجیتال را از سوی والدین و نظام تعلیم‌وتربیت جهت استفادهٔ ایمن از این فضا، مورد تأکید قرار می‌دهد.**

جدول ۱: مروری بر پیشینه تحقیق

مفاهیم نظری

مفهوم آموزش: از نظر لغوی، آموزش اسم مصدر از کلمه آموختن و به معنای یاددادن و تعلیم است. در معنای اصطلاحی، آموزش یا تعلیم به یاددادن موضوعات یا مهارت‌های خاص به فراگیران، مانند آموزش خواندن و نوشتن و... گفته می‌شود (آرمند، ۱۳۹۰: ٦٣). در تبیین مفهوم آموزش باید بیان داشت که آموزش سنگ‌بنای تکوین، حفظ و پیشرفت تمامی جوامع بشری است. همه انسان‌ها از هنگام تولد به‌گونه‌ای تحت آموزش‌های گوناگون قرار می‌گیرند، زیرا تنها از این طریق است که انسان با محیط پیرامون خود آشنا شده، فرهنگ آن را یاد می‌گیرند و برای رفع نیازهای آن جامعه، حرفه‌ای را انتخاب می‌نمایند. از منظر یونسکو، آموزش، فرآیندی است که در طی آن، چهار نوع یادگیری حاصل می‌شود: یادگیری برای زندگی‌کردن با یکدیگر، یادگیری برای دانستن، یادگیری برای انجام‌دادن امور و یادگیری برای بودن (اسنیونجو[1]، ۲۰۰۹: ۳۵۷). برای مفهوم آموزش تعاریف متعددی ارائه شده است. از نظر افلاطون، آموزش هنر ایجاد عادات خوب یا پرورش مهارت‌های فطری کسانی است که آنها را دارند. به گفته ژان ژاک روسو[2]، آموزش همزمان با مداخله و عدم مداخله ظاهر می‌شود: آموزش منفی شامل رفع هر مانعی برای رشد عادی است، باید اجازه داد که همه چیز به طور طبیعی و بدون هیچ مداخله‌ای اتفاق بیفتد. امیل دورکیم[3]، جامعه‌شناس مشهور فرانسوی، در ارائه تعریف یا اختصاص ویژگی به مفهوم آموزش منفعل نماند. بنابراین، او معتقد است که

1. Ssenyonjo
2. Jean-Jacques Rousseau
3. Émile Durkheim

تعلیم و تربیت عملی است که توسط نسل‌های بالغ بر کسانی که برای زندگی اجتماعی آماده نیستند، اعمال می‌شود. وی همچنین اظهار داشت که به نظر می‌رسد آموزش یک عمل تحریک‌آمیز عمدی است که تعداد نامحدودی از حالات فیزیکی، فکری و اخلاقی را در کودک ایجاد می‌کند (سیوربارو[1]، ۲۰۱۸: ۷۶). آموزش رسمی شامل آموزش روشمند، تدریس و آموزش توسط معلمان/ مربیان/ اساتید حرفه‌ای است؛ در حالی که آموزش غیررسمی به طور کلی شامل آموزش‌های والدین، خانواده‌ها، همسالان یا به طور کلی، تعاملات اجتماعی است. اولی شامل کاربرد آموزش (به عنوان مثال، استراتژی‌ها و/یا سبک‌های آموزشی) و توسعه برنامه‌های درسی (یعنی، مجموعه‌ای از فعالیت‌های آموزشی برای ارائه آموزش است)، در حالی که دومی شامل یادگیری اجتماعی است که فرد از تعامل خود با گروه‌های همسالان صمیمی خود به دست می‌آورد (کروس[2]، ۲۰۰۹: ۵). حق بر آموزش که از آن به حق بر تحصیل نیز یاد می‌کنند، در جهان امروز ازجمله حقوق اساسی بشری محسوب می‌شود؛ زیرا موجب شکوفایی روح، فطرت و فکر انسان می‌شود. حق بر آموزش را می‌توان حق بر بالندگی و شکوفایی که لازمه‌ی هویت و ذات انسان است، تعبیر کرد (مرندی و قربانی، ۱۴۰۰: ۸۰). همگانی‌بودن آموزش بدین معناست که تمام افراد جامعه باید قادر باشند از آن بهره‌مند شوند؛ این ویژگی با تعبیر قابلیت دسترسی شناخته می‌شود. این اصل هم دسترسی قانونی و هم دسترسی فیزیکی افراد به این حق را شامل می‌شود؛ بدین معنا که از یک سو باید تمام افراد بشر، بر اساس قوانین، حق برخورداری از آموزش را داشته باشند و هیچ قانونی نباید کسی را از این حق محروم نماید. از سوی دیگر، در عمل نیز شرایطی به گونه‌ای مهیا گردد که افراد بتوانند به امکانات و مراکز آموزشی دسترسی داشته باشند. این حق و اصول آن همواره در قانون اساسی کشورهای مختلف به رسمیت شناخته شده است و در بخش حقوق ملت در قانون اساسی ایران نیز مورد اشاره قرار گرفته و دولت نسبت به تامین امکانات حق بر آموزش و تحقق اهداف آن ملزم شده است. اصل سی‌ام و بند سوم از اصل سوم قانون اساسی، دولت را موظف به تامین وسایل آموزش‌وپرورش رایگان برای همه‌ی ملت تا پایان دوره‌ی متوسطه و ملزم به تامین وسایل تحصیلات عالی تا سرحد خودکفایی کشور به طور رایگان کرده است (صادقی رام، موذنی و پوررشید، ۱۴۰۰: ۱۶۶).

آموزش پیشگیری از جرم از طریق نهادهای آموزشی: امروزه، بیشتر قانونگذاران و سیاست‌گذاران در کنار کارکرد آموزشی محیط تحصیلی، به کارکرد پرورشی تربیتی آن نیز

1. Ciorbaru
2. Crews

توجه می‌کنند. قانونگذار ایرانی و نویسندگان شماری از مقررات فروتقنینی، در پرتو مواد ۱ و ۲ قانون اهداف و وظایف وزارت آموزش‌وپرورش ۱۳٦٦ ش، ماده ۸ قانون تشکیل شوراهای آموزش‌وپرورش در استان‌ها، شهرستان‌ها و مناطق کشور ۱۳٦۸ ش، ماده ۱ اساسنامه انجمن اولیا و مربیان ۱۳۵۸ ش، ماده ۲ اساسنامه سازمان آموزش‌وپرورش استثنایی ۱۳۷۰ ش. و اساسنامه پژوهشکده تعلیم و تربیت وابسته به آموزش‌وپرورش ۱۳۷۵ ش.، تلاش کرده‌اند وزارت آموزش‌وپرورش را به سوی اتخاذ سیاست‌ها و اجرای برنامه‌های تربیتی و پرورشی از جمله سیاست‌ها و برنامه‌های پیشگیرانه هدایت نمایند (نیازپور، ۱۳۸۵: ۷٦). سیاست‌گذاری و برنامه‌ریزی دقیق در زمینه پیشگیری از بزهکاری نیازمند تخصص دست‌اندرکاران در این خصوص و اشراف آنان به مباحث جرم‌شناختی، به ویژه مباحث پیشگیری از بزهکاری است؛ از این رو، شماری از اسناد فراملی مانند پیمان‌نامه مبارزه با فساد سال ۲۰۰۳ م. در بند ۱ ماده ۹ و مواد ۳٦ و ٦۰ به آموزش دست‌اندرکاران پیشگیری از بزهکاری اشاره کرده است. در ایران نیز با توجه به نبود تخصص در میان دست‌اندرکاران پیشگیری از بزهکاری که یکی از چالش‌های اساسی فراروی این امر به شمار می‌رود، نویسندگان پیش‌نویس برنامه ملی پیشگیری از جرم در بند «ب» گفتار چهارم و بند «الف» گفتار پنجم مبحث نخست فصل چهارم بر لزوم آموزش دست‌اندرکاران پیشگیری از بزهکاری تاکید ورزیده‌اند. به‌کارگماردن متخصصان پیشگیری از بزهکاری با آموزش دست‌اندرکاران این امر از راه برگزاری دوره‌های فراگیر می‌تواند نقش بسزایی در اتخاذ سیاست‌های دقیق در زمینه پیشگیری از بزهکاری ایفا نماید (نیازپور، ۱۳۸۵: ۷٦).

آموزش همگانی فراجا: یکی دیگر از شیوه‌های پیشگیری از جرم که سال‌هاست به طور معمول توسط نهادهای مختلف، به‌ویژه نیروی انتظامی، بکار گرفته می‌شود، آموزش‌های همگانی پیشگیری از جرم است (رضوی، ۱۳۸٦: ۱۳٤). آموزش همگانی عبارت است از مجموعه فعالیت‌هایی که به منظور یادگیری برخی از فعالیت‌های مشخص (دانش انتظامی و اجتماعی) با هدایت کارکنان معاونت اجتماعی فراجا، برای کلیه افراد جامعه انجام می‌شود. آموزش همگانی با ارتقای سطح دانش و آگاهی مهارت‌های فنی موجب بروز رفتار مطلوب به منظور کاهش فرصت‌های مجرمانه در شهروندان می‌شود (خمسه‌ای، ۱۳۸۲: ۲۰). این آموزش‌ها به عنوان یکی از مأموریت‌های ذاتی فراجا برای ایمن‌سازی اقشار مختلف اجتماع در برابر آسیب‌ها و ناهنجاری‌های اجتماعی و نهادینه‌کردن هنجارهای مثبت اجتماعی پیش‌بینی شده است. آموزش همگانی فراجا به طور مشخص دارای مأموریت و وظایف مشخصی از

شناخت علمی و دقیق پدیده‌ها و مسائل اجتماعی تا حفظ تعاملات از طریق ظرفیت‌سازی و ایجاد فرصت همکاری با اقشار مختلف اجتماعی، دستگاه‌ها و نهادهای دخیل در تولید و نگهداری نظم و امنیت اجتماعی با رویکرد جامعه‌محوری در فراجا است که در ماده ٤ بند ۱۸ قانون فراجا مصوب ۱۳٦۹ به عنوان یکی از وظایف فراجا اشاره شده است. در حال حاضر، سازمان و تشکیلات آموزش همگانی زیرمجموعه معاونت فرهنگی و اجتماعی فراجا است (بیگی راد، ۱٤۰۲: ۸۳). آموزش همگانی نوعی آموزش است که حداقل دارای این ویژگی‌ها باشد: ۱- برای عموم افراد جامعه باشد، ۲- منجر به افزایش سطح آگاهی‌های جامعه هدف شود، ۳- سازمان‌یافته و هدفمند باشد، ٤- پاسخی به نیاز جامعه باشد، ۵- منجر به رضایت‌مندی بیشتر افراد جامعه گردد (سهل آبادی، ۱۳۸۷). پلیس فتا به عنوان پلیس تخصصی مبارزه با جرائم سایبری در قالب آموزش همگانی با تولید و اکران مستندات آموزشی مختلف و متنوع در قالب انیمیشن و موشن‌گرافیک، پادکست، اینفوگرافی، فیلم‌های کوتاه و برگزاری انواع کلاس‌های آموزشی در سطوح مختلف اقشار جامعه درصدد افزایش آگاهی و دانش عمومی کاربران از آسیب‌ها و تهدیدات فضای مجازی برآمده است.

بزه‌دیدگی سایبری و انواع جرائم سایبری: قربانی‌شدن ممکن است در پی یک عامل غیرانسانی (طبیعت، حیوانات و...) رُخ دهد، همچنان که امکان دارد از رهگذر رفتار مجرمانه انسانی روی دهد؛ عمل قربانی‌کردن مجرمانه را بزه‌دیدگی گویند (قاسمی و مرادی، ۱۳۹۸: ۱۵٦). عمل مجرمانه، هر رفتاری اعم از فعل یا ترک فعل است که توسط قانون ممنوع اعلام شده (هم برای بزه‌دیده و هم برای بزه‌کار) و برای آن مجازات تعیین شده است. اصطلاح بزهکاری سایبری هنوز موضوع تعریفی رسمی، چه در اسناد بین‌المللی و چه در قوانین بسیاری از کشورها، قرار نگرفته است. این متون با تکیه بر رویکردی کاربردی، ترجیح می‌دهند به‌جای ارائه تعریفی قانونی، محتوای این بزهکاری را تبیین کرده و جرائم تشکیل‌دهنده آن را دسته‌بندی کنند (کرد علیوند و میرزایی، ۱۳۹۷: ۱۹۲)؛ اما در یک تعریف کلی، جرائم سایبری را هر گونه فعالیتی که در آن رایانه‌ها یا شبکه‌ها، ابزارها، هدف یا مکانی برای فعالیت تبهکاری باشد، توصیف کرده‌اند (گرکی[1]، ۱۳۸۹: ۳۲). کنوانسیون بوداپست[2] چهار دسته از جرائم ارتکابی از طریق سیستم‌های رایانه‌ای و فناوری اطلاعات را تعریف می‌کند. این کنوانسیون جرائم سایبری را در چهار دسته به شرح زیر دسته‌بندی کرد:

1. Gercke
2. the Budapest Convention

۱. جرائم علیه محرمانه‌بودن:[1] صحت، یکپارچگی[2] و در دسترس‌بودن داده‌ها و سیستم رایانه‌ای که شامل دسترسی و مداخله غیرقانونی، در داده‌ها، دستگاه‌ها و سیستم شبکه به طور کلی، شنود غیرقانونی[3]، سوءاستفاده از دستگاه‌ها که شامل فروش، سرقت و... غیرقانونی دستگاه، رمز عبور و غیره می‌شود (عنوان ۱ کنوانسیون).

۲. جرائم مرتبط به رایانه:[4] که شامل جعل مرتبط با رایانه[5] می‌شود و ممکن است منجر به تولید داده‌های غیرمعتبر برای سود غیرقانونی و فریب دیگران و کلاهبرداری رایانه‌ای[6] شود؛ همچنین، امکان دارد باعث زیان از جمله ضرر مالی در مقیاس وسیع برای دیگران شود (عنوان ۲ کنوانسیون).

۳. جرائم مرتبط با محتوا:[7] که شامل جرائم مرتبط با هرزه‌نگاری کودکان[8] می‌شود (عنوان ۳ کنوانسیون).

٤. جرائم مرتبط با نقض حق نشر و حقوق مرتبط[9] (عنوان ٤ کنوانسیون). (هالدر[10]، ۱٤۰۲: ۳۸).

روش

پژوهش حاضر از نظر هدف، کاربردی و به لحاظ گردآوری داده، به روش کتابخانه‌ای و از طریق مطالعه منابع معتبر انجام شده و اطلاعات بدست‌آمده به صورت توصیفی- تحلیلی مورد تجزیه‌وتحلیل قرار گرفته است.

یافته‌ها

ایجاد دانش بنیادی: آموزش سنگ‌بنای ایجاد دانش اساسی در خصوص ملزومات زندگی اجتماعی انسان به‌ویژه در رابطه با امنیت سایبری و زیست مجازی است. معرفی مفاهیم ایمنی سایبری در سنین پایین از طریق برنامه‌های درسی مدارس، بنیادهای اولیه ایمنی آنلاین را در دانش‌آموزان ایجاد می‌کند. با القای اهمیت رمزهای عبور قوی در دنیای دیجیتال و آموزش شناخت انواع حملات سایبری و نحوه مقابله با آنها و همچنین، یادگیری نحوه حفاظت از

1. Confidentiality
2. Integrity
3. Illegal Interception
4 .Computer Related Offences
5. Computer Related Forgery
6. Computer Fraud
7. Content Related Offences
8. Child Pornography
9. Copyright Infringement And Related Rights
10. Halder

رایانه‌ها و داده‌های شخصی، به تدریج رفتار سایبری ایمن در دانش‌آموزان ایجاد می‌شود که می‌تواند برای در طول زندگی از وی در مقابل تهدیدات سایبری محافظت نماید. نتایج تحقیقات در بین دانش‌آموزان ۸ تا ۱۰ ساله نشان می‌دهد که برنامه آگاهی از امنیت سایبری مؤثر است و بر رفتار آنلاین دانش‌آموزان تأثیر می‌گذارد (الشمسی[1]، ۲۰۱۹: ۲۸). در حالی که در مورد نیاز به آموزش امنیت سایبری اتفاق‌نظر وجود دارد، دیدگاه‌های متفاوتی در مورد سنی که این آموزش باید آغاز شود و مسئولیت اصلی ارائه آن برعهده چه کسی باشد، وجود دارد (مورنو[2] و همکاران، ۲۰۱۳: ۱). برخی از کارشناسان معتقدند که والدین باید در درجه اول ایمنی اینترنت را آموزش دهند، در حالی که برخی دیگر بر نقش مربیان تأکید دارند.

بالابردن سطح سواد دیجیتال عمومی: سواد دیجیتال بر توانایی فرد در درک متون چندرسانه‌ای و توانایی دسترسی، مدیریت، درک، ادغام، ارتباط، ارزیابی و ایجاد اطلاعات ایمن و مناسب از طریق فناوری‌های دیجیتال و ارائه سطح مشخصی از امنیت در فضای دیجیتال اشاره دارد و شامل مهارت‌هایی است که به گونه‌های مختلف با عناوینی همچون سواد رایانه‌ای، سواد فناوری اطلاعات و ارتباطات، سواد اطلاعاتی و سواد رسانه‌ای شناخته می‌شوند (موسسه آمار یونسکو[3]، ۲۰۱۸: ٦). سواد دیجیتال اغلب بجای مفاهیمی مانند سواد سایبری، سواد رایانه‌ای و سواد رسانه‌ای بکار می‌روند، در حالی که مفاهیم متمایز و در عین حال به‌هم‌پیوسته‌ای هستند که در مطالعات امنیت سایبری مورد استفاده قرار می‌گیرند. سواد دیجیتالی مهارت‌های اساسی را برای استفاده از فناوری‌های دیجیتال فراهم می‌کند، در حالی که سواد سایبری و سواد رایانه‌ای بر این پایه استوار است تا به چالش‌های امنیتی ذاتی در محیط‌های دیجیتال پاسخ دهد؛ با این حال، هر دو برای محافظت از خود در عصر دیجیتال ضروری هستند و جزء لاینفک امنیت سایبری محسوب می‌شود. پژوهش‌های متعدد نشان می‌دهد که میان سواد دیجیتال و ابعاد بزه‌دیدگی در فضای مجازی رابطه معنی‌دار وجود دارد (ابراهیمی، صابری و لکی، ١٤٠٢: ٦٩). آموزش در افزایش سواد دیجیتال و آگاهی سایبری بسیار موثر است. از طریق برنامه‌های آموزشی ساختاریافته و برنامه‌های درسی است که دانش‌آموزان یاد می‌گیرند از حریم خصوصی خود محافظت کنند و تهدیدات سایبری را تشخیص دهند. در همین راستا، مطالعات زیادی بر نیاز به آموزش جامع و ارتقای سطح سواد دیجیتال و سایبری به منظور آماده‌سازی افراد برای پیچیدگی‌ها و مقابله با تهدیدات عصر

1. Al Shamsi
2. Moreno et al
3. UNESCO Institute for Statistics

دیجیتال تأکید می‌کنند (سیدین بروجنی، موذن و بهشتی، ۱۴۰۲: ۱، مرشدی و آل رسول، ۱۴۰۲: ۶۰؛ صیادی و همکاران، ۱۴۰۱: ۲۷). در حالی که اهمیت سواد دیجیتال در سطوح مختلف آموزشی و در کشورهای مختلف شناخته شده است، پیاده‌سازی و ادغام برنامه‌های آموزشی سواد دیجیتال و امنیت سایبری به طور قابل‌توجهی متفاوت است. کشورهای توسعه‌یافته تمایل دارند بر جمعیت سالمندان تمرکز کنند، در حالی که کشورهای در حال توسعه افراد با مهارت‌ها و سطح تحصیلات پایین را در اولویت قرار می‌دهند.

افزایش رفتار مسئولانه آنلاین: ویژگی‌های خاص فضای سایبر از جمله امکان گمنامی و کسب هویت‌های گوناگون مجازی، فرامکانی و عدم نیاز به مواجهه حضوری، سیالیت و غیرملموس‌بودن و امکان نامرئی‌بودن، عوامل بازدارنده فردی و اجتماعی را تضعیف می‌کنند. از این رو، کاربران در زیست مجازی رفتارهایی را بروز می‌دهند که در زیست حقیقی از بروز آن خودداری می‌کردند (سولر[1]، ۲۰۰۴: ۳۲۳). نتایج تحقیقات مختلف (سولر۲۰۰۴؛ جایشانکار: ۲۰۰۸؛ آگوستینا: ۲۰۱۲) در مورد رفتارهای کاربران معمولی اینترنت نشان می‌دهد که افراد در فضای سایبری چیزهایی را می‌گویند و انجام می‌دهند که معمولاً در روابط رودررو نمی‌گویند یا انجام نمی‌دهند (آگوستینا[2]، ۲۰۱۵: ۴۲). شرایط روانی خلوت، عدم احساس خطر و ویژگی ناشناس، یک حس تحریک، غلیان احساسی و فقدان مسئولیت منجر به ولنگاری در شخص پدید می‌آورد که موجب کاهش محدودیت‌های درونی و فقدان علقه‌های اجتماعی یا خودارجمندی می‌شود (حسنی، ۱۳۸۸: ۷۵). این امر به نوبه خود می‌تواند کاربر را در معرض مجرمان سایبری قرار دهد و در نهایت، با وارونگی نقش وی همراه شده و موجبات بزه‌دیدگی او را فراهم آورد. بنابراین، رفتار آنلاین مسئولانه و اخلاقی در فضای سایبری برای مصون‌ماندن از حملات سایبری احتمالی بسیار حایز اهمیت است.

رفتار آنلاین مسئولانه در فضای مجازی طیفی از اقدامات و ملاحظات ایمنی- اخلاقی را در بر می‌گیرد که شامل شناخت اهمیت اینترنت و تأثیرات واقعی تعامل آنلاین بر کاربران، مشارکت در اقداماتی که به ثبات و امنیت فضای مجازی کمک می‌کند و آگاهی از سیال‌بودن هویت در محیط‌های مجازی و پیامدهای آن در دنیای حقیقی می‌شود. آموزش اخلاق سایبری به دلیل تأثیر عمیق آن بر افراد، جامعه و بستر دیجیتال قابل‌توجه است، زیرا تصمیم‌گیری اخلاقی، رفتار آگاهانه و استفاده مسئولانه از فناوری را تقویت می‌کند. با آموزش افراد در مورد ابعاد اخلاقی فضای مجازی، آنها از پیامدهای بالقوه اقدامات خود آگاه می‌شوند و حس

1. Suler
2. Agustina

شهروندی دیجیتال را در خود پرورش می‌دهند؛ علاوه بر این، آموزش اخلاق سایبری، امنیت و حریم خصوصی آنلاین را ارتقا می‌دهد، زیرا افراد در مورد اهمیت حفاظت از اطلاعات شخصی و حفظ یک حضور آنلاین امن می‌آموزند (شانتوش و تیاگو[1]، ۲۰۲٤: ۳٤). آموزش با القای درک اخلاقی و رویکرد همدلانه نسبت به دیگران، به مبارزه با آزارواذیت سایبری، رفتار مخرب آنلاین و جرائم سایبری کمک می‌کند.

توسعه مهارت‌های تفکر انتقادی: عصری که در آن به سر می‌بریم، عصر داده‌هاست و جهان در حال گذر از جامعه‌ای با ساختارهای سنتی به جامعه‌ای مبتنی بر فناوری اطلاعات می‌باشد؛ اجتماعی که در آن، ریزپردازنده‌ها می‌توانند حجم عظیمی از اطلاعات را در مدت زمان بسیار کوتاه پردازش کنند و کابل‌های اینترنت فیبر نوری امکان انتقال داده‌ها را با سرعت صدها مگابایت در ثانیه فراهم کنند (هابیروس[2]، ۲۰۱۸: ۲). با ادامه رشد و گسترش دنیای دیجیتال، تهدیدات امنیت آنلاین پیچیده‌تر می‌شوند و بشر در عصر دیجیتال با مقدار بسیار وسیعی از داده‌ها مواجه است که بعضاً، می‌توانند غیرصحیح، مشکل‌زا و خطرآفرین باشند. از آنجا که مجرمان فعالیت‌های خود را با موقعیت جدید سازگار کرده‌اند و از تکنیک‌های مهندسی اجتماعی و حملات سایبری مبتنی بر اصول روان‌شناختی برای فریب و دستکاری ادراک افراد و به‌دست‌آوردن اطلاعات ارزشمند به صورت ماهرانه بهره می‌برند (کورادینی و ناردلی[3]، ۲۰۲۰: ۵۹)، تفکر انتقادی یک مهارت ضروری برای پیشگیری از جرائم سایبری است. جامعه مدرن نیازمند آگاهی و سطح بالایی از تفکر انتقادی برای تضمین ایمنی جمعیت در دنیای مدرن است. فکر انتقادی در امنیت سایبری شامل فرآیند تجزیه‌وتحلیل، ارزیابی و تفسیر داده‌ها برای تصمیم‌گیری آگاهانه می‌شود. این امر مستلزم آن است که افراد در مورد اطلاعاتی که به آنها ارائه می‌شود، عمیقاً فکر کنند، مفروضات و سوگیری‌ها را زیر سوال ببرند و قبل از قضاوت یا اقدامی، چندین دیدگاه را در نظر بگیرند. توانایی تفکر انتقادی به افراد این امکان را می‌دهد تا اطلاعات و موقعیت‌ها را ارزیابی کنند، تهدیدات و آسیب‌پذیری‌های بالقوه را شناسایی کنند و تدابیر مؤثری برای کاهش این خطرات ایجاد کنند (کوریلو و همکاران[4]، ۲۰۲۳: ۷۲؛ آیس برگ[5]، ۲۰۲۳). تحقیقات از اثربخشی برنامه‌های آموزشی بر تفکر انتقادی حکایت دارند (زینالی[6] و همکاران، ۲۰۱۹: ۲۱۳). پرورش تفکر انتقادی در نوجوانان و جوانان

1. Santhosh & Thiyagu,
2. Habirovs
3. Corradini & Nardelli
4. Kurylo et al
5. Iceberg
6. Zeniali et al

به آنها کمک می‌کند نه تنها دانش کسب کنند، بلکه به تجزیه‌وتحلیل، درک و ارزیابی انتقادی اطلاعاتی که در دنیای آنلاین با آنها مواجه می‌شوند، کمک می‌کند. محققان تاکید می‌کنند که آموزش و توسعه تفکر انتقادی ابزار مهمی برای جلوگیری از جرائم سایبری ازجمله فیشینگ و تضمین امنیت اطلاعات افراد است (سارکر و همکاران[1]، ۲۰۲٤: ۱؛ کوریلو و همکاران، ۲۰۲۳: ۷۰).

پرکردن شکاف دانش: اجتماعی‌سازی مجازی از طریق توسعه شبکه‌های اجتماعی امکان حضور عموم مردم را در فضای مجازی فراهم آورده است و بسیاری برای انجام فعالیت‌های روزمره به این فضا وابسته هستند. بنابراین، کاربران در هر سطح دانش و تخصصی که باشند، در جهان مدرن نمی‌توانند خود را نسبت به امکانات دیجیتال بی‌علاقه و بی‌تفاوت نشان دهند؛ اما شکاف دیجیتالی بین بومیان دیجیتال (افرادی که پیرامون فناوری‌های دیجیتال متولد شده‌اند) و مهاجران دیجیتالی (افرادی که قبل از سال ۱۹٦٤ در دنیای قبل از کامپیوتر به دنیا آمده‌اند[2]) تفاوت بین آگاهی و آشنایی هر نسل از اینترنت را برجسته می‌کند (زور[3]، ۲۰۱۱: ۱۱). ممکن است برخی از مهاجران دیجیتال مخصوصاً، افراد با سطح تحصیلات پایین، نتوانند خود را با فناوری‌های همیشه در حال تغییر و پیشرفت همگام و سازگار کنند. این شکاف موجود بین کابران و سواد دیجیتال و دانش امنیت سایبری به ویژه در بین میانسال و سالمندان، موج شدیدی از بزه‌دیدگی‌ها را به دنبال دارد. از این رو، افراد مسن نیازمند منابع آگاهی سایبری خاصی هستند. کاراگیانوپولوس[4] و همکارانش (۲۰۲۱) بر این باور هستند که آموزش در رابطه با خطرات سایبری و پیشگیری بسیار مهم است، اما تنها زمانی می‌تواند موثر باشد که متناسب با نیاز و مشارکت کسانی که قرار است این آموزش را به صورت جمعی دریافت کنند، طراحی شود. بنابراین، برنامه‌های آموزش ایمنی سایبری بایستی متناسب با نیازها و خصوصیات گروه‌های هدف طراحی گردد تا به اهداف پیشگیرانه نایل آیند.

تقویت نظارت والدین: آشنایی والدین با این فضا و داشتن تحصیلات و سواد رایانه‌ای در سطح قابل‌قبول از شاخص‌های مهم در محیط خانواده است که می‌تواند نقش اساسی در کاهش یا افزایش میزان بزه‌دیدگی سایبری کودکان که بزرگسالان آینده هستند، داشته باشد. نفوذ والدین در کودکان تنها جنبه ارثی ندارد، بلکه در آشنایی کودک با زندگی اجتماعی و

1. Sarker et al

۲. این معیار برای کشورهای صنعتی است. در ایران، ظهور و بکارگیری ابزار الکترونیکی در سطح گسترده به اوایل دهه ۸۰ شمسی برمی‌گردد.

3. zur
4. Karagiannopoulos et al

جامعه‌پذیرشدن وی، نقش مؤثری را ایفا می‌کند؛ اما بسیاری از والدین با توجه به اختلاف سنی و شرایط متفاوت دوران رشد و تفاوت‌های فاحش ارزشی حاکم بر دنیای آنها با دنیای فرزندان خود، از آسیب‌ها و فرصت‌های شبکه مجازی غافلند؛ لذا، قادر به مدیریت و درک درست رفتارهای فرزندان خود نبوده و این عامل باعث تشدید در معرض آسیب قرارگرفتن فرزندان می‌شود (چاوشی و کرامتی معز، ۱۳۹۷:۱۱۱). بسیاری از تحقیقات تاثیر نقش آموزشی و نظارتی والدین در آموزش سواد دیجیتال و رفتار اخلاقی و مسئولانه به کودکان و مدیریت خطرات پیش روی آنان در فضای سایبر را تایید کردند (مهرپارسا[1]، ۱۴۰۰: ۳۵؛ دانیلا و رودلفا[2]، ۲۰۱۸: ۱۰۴). از این رو، اجرای برنامه‌های آموزشی برای والدین می‌تواند در تقویت نقش نظارتی و آموزشی والدین کارآمد باشد.

افزایش مشارکت اجتماعی: توسعه، کارآمدی و اجرای موفقیت‌آمیز سیاست‌های پیشگیری از جرائم، ارتباط تنگاتنگی با جلب همکاری عموم مردم دارد. مقابله با بزه سایبری فراتر از ظرفیت نهادهای رسمی عدالت کیفری و مستلزم مشارکت عموم شهروندان یا کاربست سیاست جنایی مشارکتی است. پژوهشگران تدابیری همچون «دعوت از افراد شریف برای حضور اثرگذار در فضای مجازی»، «تشکیل گروه‌های گشت‌زنی خصوصی»، «تقویت هنجارهای بر خط»، «تفویض قسمتی از امر تعقیب به سازمان‌های مردم‌نهاد» و «استفاده از هیئت منصفه در جریان دادرسی» را به عنوان گزینه‌های یک راهبرد مشارکتی در کنترل و مقابله با جرائم سایبری معرفی می‌کنند (سلیمی قلعه، ۱۴۰۱: ۲۷۳). یکی از جنبه‌های حیاتی آموزش، تربیت نیروی انسانی متخصص و توانمندسازی اعضای جامعه و تقویت سازمان‌های مردم‌نهاد برای اجرای سیاست‌های مشارکتی است.

تربیت نیروی انسانی متخصص: به علت ماهیت فنی و تخصصی جرائم سایبری، کشف جرم، تعقیب بزهکاران و رسیدگی به ادله الکترونیکی نیازمند نیروی انسانی متخصص در نهادهای کیفری مبارزه با جرم است. الگوهای بزه‌دیدگی سایبری گسترش یافته است. آنها کل سیستم پلیسی را مجبور کرده‌اند که مسیر جدیدی را در کنترل جرم و جنایت در پیش بگیرد. با کنوانسیون اتحادیه اروپا در مورد جرائم سایبری در سال ۲۰۰۱، الگوهای برجسته جرائم سایبری به رسمیت شناخته شد. این کنوانسیون توصیه کرد که آموزش پلیس و دستگاه عدالت کیفری باید متمرکزتر و تخصصی‌تر باشد و در عین حال، باید ماهیت پیشگیرانه و اصلاحی داشته باشد (هالدر، ۲۰۲۲: ۴۷). میزان نیروی تخصصی برای پیشگیری از جرائم سایبری و

1. Mehrparsa
2. Daniela & Rudolfa

میزان تخصص آن‌ها با سطح پیشرفت و توسعه کشورها ارتباط چشمگیری دارد؛ به عبارت دیگر، هرچه توسعه‌یافته‌تر باشد و زیرساخت‌های قوی‌تری داشته باشد، سرمایه و نیروی تخصص‌یافته‌تری برای صیانت از حریم سایبری خود اختصاص می‌دهد؛ و در مقابل، کشورهایی که با مشکل اقتصادی بیشتری مواجه هستند، سهم کمتری در این قضیه دارند. بر اساس گزارش سازمان ملل، کشورهایی که سطح کمتری از توسعه‌یافتگی را تجربه کرده‌اند، تقریباً به ازای هر ۱۰۰ هزار نفر کاربر ملی اینترنت، ۰/۲ نیروی پلیس سایبری اختصاص داده‌اند؛ در حالی که در کشورهای توسعه‌یافته، ۲ تا ۵ درصد بیشتر است (فرهادی آلاشتی، ۱۳۹۵: ۱٦٥). نهادهای آموزش در تربیت و تامین نیروهای متخصص مورد نیاز پلیس فتا و دادسراها و دادگاه‌های تخصصی رسیدگی به جرائم سایبری نقش اساسی دارد.

توانمندسازی قربانیان: توانمندسازی قربانیان جرائم سایبری از طریق تدابیر آموزشی از دو منظر حایز اهمیت است: ۱.پیشگیری از بزه‌دیدگی دوباره و مکرر؛ ۲. جلوگیری از بزه‌دیدگی ثانویه و کاهش رقم سیاه جرائم.

اصطلاح بزه‌دیدگی دوباره را می‌توان ناظر بر مواردی دانست که شخص برای دومین بار بزه‌دیدگی را تجربه می‌کند، اما هرگاه بزه‌دیدگی فرایند پیوسته‌ای باشد که در پی آن، درد و رنج حاصل شود، می‌توان از بزه‌دیدگی یا بزه‌دیدگی‌های مکرر سخن به میان آورد (رجبی، ۱۳۸۸: ١٦). در صورتی که بزه‌دیده یک جرم برای بار دوم قربانی شود، نشانه‌ای از آسیب‌پذیری است و نشان می‌دهد که بزه‌دیده بیش‌ازحد در معرض خطر قرار دارد. فضای سایبر از آنجا که مبتنی بر طبیعتی خودکار است، لذا توانایی نگهداری و باقی‌نگهداشتن ابزار یا آثار واقعی مجرمانه را به میزان بالایی داراست. از طرف دیگر، مرتکب می‌تواند با استفاده از امکانات فنی که در اختیار دارد، در برخی موارد جرم را تا بی‌نهایت تکرار کند؛ این بدان علت است که عمل فیزیکی که مجرم انجام می‌دهد، یک بار انجام می‌شود، اما رایانه به طور خودکار آن را تکرار می‌کند (زیبر، ۱۳۸۳: ٦٩). آموزش یک عنصر کلیدی در پیشگیری از قربانی‌شدن دوباره و مکرر جرائم سایبری است، زیرا علاوه بر آموزش الگوهای بزه‌دیدگی، عوامل بزه‌دیده‌ساز، رخنه‌های امنیتی موجود در سیستم، برای بزه‌دیده این امکان را محیا می‌کند شیوه‌های خودمحافظتی و نحوه برخود با حملات سایبری را فرا بگیرد و در مواجهه با حملات آتی بکار ببندد.

بزه‌دیدگی دوم شامل ناملایماتی می‌شود که از رهگذر پاسخگویی افراد (مانند اعضای خانواده و دوستان بزه‌دیده) یا برخی از نهادها (به‌ویژه نظام عدالت جنایی، پلیس، دادسرا،

دادگاه و...) به بزه‌دیده وارد می‌شود. بزه‌دیدگان اغلب برای فرار از این ناملایمات تصمیم می‌گیرند بزه‌دیدگی خود را گزارش نکنند که به نوبه خود، بالارفتن رقم سیاه جرائم را به دنبال دارد. یکی از چالش‌های عمده در پیشگیری از بزه‌دیدگی سایبری، سکوت بزه‌دیده به دلیل عدم آگاهی از حقوق خود در فرآیند دادرسی و یا دلسردی وی از حصول نتیجه و احقاق حق می‌باشد (هالدر، ۲۰۲۲: ۹). برنامه‌های آموزشی با آگاهی‌بخشی به کاربران در رابطه با حقوق آنان در مراحل دادرسی و خطرهایی که ممکن است در نتیجه سکوت بعدها گریبان‌گیرشان شود، افراد را به گزارش حوادث سایبری برای شناسایی و کاهش سریع تهدیدات تشویق می‌کنند.

بحث و نتیجه‌گیری

همزمان با نهادینه‌شدن بیشتر فناوری اطلاعات در جوامع، جرائم سایبری به عنوان پیامد منفی و جنبه تاریک فضای سایبر به‌صورت فزاینده‌ای تهدیدات قابل‌توجهی را برای افراد، سازمان‌ها و دولت‌ها ایجاد می‌کنند. این درحالیست که اقدامات سنتی در مبارزه با جرائم سایبری اغلب با چالش‌های گوناگونی روبرو هستند و رویکردهای نوین نیز بیشتر بر پیشگیری فناورانه تمرکز دارند و اغلب عامل انسانی، یعنی تجربیات و آسیب‌پذیری‌های بزه‌دیدگان در طراحی راهبردهای پیشگیرانه نادیده گرفته می‌شوند. تحقیقات متعدد نشان می‌دهند که ناآگاهی از ویژگی‌های اصلی بزه‌دیدگان سایبری و از عوامل اصلی بزه‌دیدگی سایبری است. فضای سایبر، فضایی جدید و مدرنی است و بالتبع، تهدیدات و جرائمی که در این فضا شکل می‌گیرند نیز نوظهور خواهند بود. بنابراین، حضور ایمن در این محیط و مقابله با تهدیدات آن نیاز به آگاهی و دانش رایانه‌ای دارد. امروزه، افراد در هر سطح دانش و تحصیلاتی که باشند، نمی‌توانند خود را نسبت به امکانات و جذابیت‌های فضای مجازی بی‌علاقه و بی‌تفاوت نشان دهند. از این جهت، فراگیری نحوه صحیح استفاده از این امکانات و مقابله با تهدیدات از ملزمات کاربری در فضای سایبر است. برخی از مفسران اظهار داشته‌اند که ظهور «فضای سایبری» نشانگر ایجاد یک محیط اجتماعی جدید با ساختارهای هستی‌شناختی و معرفت‌شناختی، محدودیت‌ها و امکانات، متمایز است. در این فضای اجتماعی متناوب، اشکال جدید و متمایز تلاش مجرمانه ظهور می‌کند و نمی‌توان با آموزش‌های سنتی این دانش را به کودکان تعلیم داد. با توجه به بررسی‌های انجام‌شده، آموزش به‌عنوان یکی از مؤثرترین راهکارها در پیشگیری از بزه‌دیدگی سایبری مطرح می‌شود. آموزش، افراد را با خطرات و تهدیدات فضای مجازی آشنا کرده و مهارت‌های لازم برای مقابله با آن‌ها را به آن‌ها می‌آموزد. این امر موجب افزایش آگاهی و تغییر رفتار افراد در فضای مجازی شده و درنتیجه، احتمال بزه‌دیدگی را کاهش می‌دهد. آموزش در حوزه پیشگیری از بزه‌دیدگی سایبری باید به گروه‌های مختلف جامعه ارائه شود. کودکان و نوجوانان، والدین، معلمان و عموم مردم همگی نیازمند آموزش‌های متناسب با نیازهای خود هستند. خانواده به عنوان اولین و مهم‌ترین نهادی که کودک در آن، فرآیند اجتماعی‌شدن را طی می‌کند و والدین به عنوان بازیگران اصلی این نهاد، نقش آموزشی خاصی را می‌توانند داشته باشد؛ اما بسیاری از والدین با توجه به اختلاف سنی و شرایط متفاوت دوران رشد خود و تفاوت‌های فاحش ارزشی حاکم بر دنیای آنها با دنیای فرزندان خود، از آسیب‌ها و فرصت‌های شبکه مجازی غافلند. با توجه به دانش رایانه‌ای کم و سطح تحصیلات پایین والدین، بیشتر بار

آموزشی کودکان به عهده نهادهای دولتی متولی آموزش، چون مدرسه و دانشگاه‌ها، می‌افتد. مدارس به عنوان اولین نهاد آموزش نظام‌مند که انسان‌ها با آن مواجه می‌شوند، نقش حیاتی در آموزش مهارت‌های مورد نیاز برای زیست ایمن در دنیای مدرن و دیجیتالی‌شده و ایجاد دانش بنیادی، آموزش رفتار مسئولانه آنلاین و توسعه مهارت‌های تفکر انتقادی نسبت به مسایل نوظهور در کودکان و نوجوانان را دارند. از این رو، در کشورهای توسعه‌یافته ایمنی سایبری در برنامه‌های درسی مدارس گنجانده شده است. در ایالات متحده، سازمان‌های دولتی مانند آژانس امنیت سایبری و امنیت زیرساخت[1] و موسسه ملی استاندارد و فناوری[2] منابع ضروری از جمله کتب و طرح‌های درسی را با هدف آموزش مهارت‌های محافظت از رمز عبور و حریم خصوصی و تشخیص فیشینگ به دانش‌آموزان و مربیان مدارس ابتدایی و متوسطه ارایه می‌دهد. دولت بریتانیا نیز علاوه بر گنجاندن ایمنی سایبری در کتب درسی مدارس با برنامه‌ای تحت عنوان «سایبرفرست[3]» که توسط مرکز ملی امنیت سایبری[4] راهبری می‌شود، دانش‌آموزان را از سنین ۱۱ سالگی برای مواجه با چالش‌های دنیای دیجیتال آماده می‌کند. با این وجود، در ایران به دلیل نبود راهبرد، عدم تخصیص بودجه کافی و فقدان نیروی انسانی آموزش‌دیده تاکنون برنامه خاصی در مدارس جهت آموزش امنیت سایبری در نظر گرفته نشده است.

از سوی دیگر، بخش بزرگی از جامعه مانند میانسالان و سالمندان، فرصت حضور در نهادهای آموزشی را ندارند. از این جهت، کمپین‌های آگاهی عمومی و آموزش‌های همگانی می‌توانند با قابلیت تغییر الگوهای عمومی رفتار آنلاین و ترمیم شکاف دانش دیجیتال ایجادشده، در برنامه‌های پیشگیری از جرائم حایز اهمیت زیادی باشند. یکی از ابتکارات شاخص در این خصوص، «**ماه امنیت سایبری اروپا**[5]» است که توسط آژانس امنیت سایبری اتحادیه اروپا و کمیسیون اروپا هر ماه اکتبر در کشورهای عضو برگزار می‌شود. کمپین «قبل از کلیک فکر کنید[6]» با ترویج بررسی منبع پیام‌ها، اجتناب از کلیک بر روی لینک‌ها مشکوک و از منابع ناشناس با یادآوری دائمی از مسئولیت شخصی در محافظت از خود، تاثیر گسترده‌ای در ارتقای رفتار مسئولانه آنلاین در سطح اتحادیه اروپا داشته است. در ایران، تلاش‌هایی توسط نهادهایی همچون مرکز ملی فضای مجازی و پلیس فتا در این زمینه انجام پذیرفته است. با این وجود، طراحی و اجرای کمپین‌هایی مستمر در سطح ملی مشاهده نمی‌شود. از این منظر،

1. Cybersecurity and Infrastructure Security Agency
2. National Institute of Standards and Technology
3. CyberFirst
4. National Cyber Security Centre
5. European Cybersecurity Month
6. ThinkB4UClick

وضعیت کمپین‌های ارتقای ایمنی سایبری در ایران از جهت آگاهی‌بخشی عمومی، ضعیف و ناکافی به نظر می‌رسد.

وجود نیروی انسانی متخصص یک مولفه اساسی در موفقیت برنامه‌های پیشگیری از جرائم به شمار می‌رود. برنامه «**ابتکار ملی برای آموزش امنیت سایبری**[1]» که یک برنامه مشارکتی بین دولت، دانشگاه‌ها و بخش خصوصی در ایالات متحده است، با هدف تقویت آموزش و توسعه نیروی کار در بخش امنیت سایبری طراحی شده است و چارچوب مهارت‌ها، دانش و وظایف مشاغل امنیت سایبری را استانداردسازی کرده و مسیر آموزشی مشخصی از سطح مبتدی تا حرفه‌ای را ارایه می‌دهد و از طریق همکاری با بخش‌های مختلف با برگزاری کنفرانس و کارگاه‌های آموزشی، به توسعه منابع آموزشی و تربیت نیروی متخصص کمک می‌کند؛ اما در ایران، برنامه‌های آموزش سایبری اغلب پراکنده و فاقد یک چارچوب ملی جامع است. از سوی دیگر، آموزش افسران پلیس و مقامات قضایی برای ردیابی و رسیدگی به مدارک دیجیتالی، به علت ماهیت چندرشته‌ای این مشاغل، از چالش‌های عمده دولت‌ها در مواجهه با جرائم سایبری است؛ زیرا در کنار تسلط به ابعاد فنی، نیازمند دانش حقوقی، مهارت‌های انتظامی و حتی درک روان‌شناختی و جامعه‌شناختی از موضوع است. جرم‌شناسی سایبری یک رشته نوظهور چندشاخه‌ای است که تحقیقات رشته‌های مختلفی مانند جرم‌شناسی، بزه‌دیده‌شناسی، جامعه‌شناسی، علوم اینترنت و علوم کامپیوتر را دربرمی‌گیرد. در حالی که کشورهای مختلف از جمله هند، از ظرفیت‌های این رشته علمی برای تربیت نیروی انسانی مورد نیاز خود بهره می‌برند، تاسیس رشته مستقل جرم‌شناسی سایبری که آمیزه‌ای از مطالب فنی و نظری باشد، در دانشگاه‌های ایران در آینده‌ای نزدیک، دور از دسترس به نظر می‌رسد.

در نهایت، آموزش‌های امنیت سایبری بایستی به صورت مداوم و مستمر و با استفاده از روش‌های متنوع انجام پذیرد تا بتواند تاثیر بیشتری در جامعه داشته باشد. از این رو، همکاری بین نهادهای مختلف از جمله دولت، مدارس، دانشگاه‌ها، رسانه‌ها و نهادهای انتظامی و کیفری برای تدوین و اجرای راهبرد جامع و کارآمد برای تربیت نیروی انسانی متخصص و آموزش مهارت‌های پیشگیری از جرائم سایبری در جهت تربیت شهروندان دیجیتال مسئول، ضروری است. با توجه به یافته‌های این پژوهش، در طراحی و اجرای برنامه‌های آموزش‌محور پیشگیری از بزه‌دیدگی سایبری باید نکات زیر مورد توجه قرار گیرد:

1. National Initiative for Cybersecurity Education (NICE)

- آموزش‌های منظم و مستمر، سطح آگاهی افراد را نسبت به خطرات و تهدیدات سایبری به‌طور چشمگیری افزایش می‌دهد. از این رو، سیاست‌های اتخاذی بایستی استمرار برنامه‌های آموزشی را تضمین نماید.
- گروه‌های مختلف جامعه با توجه به ویژگی‌های فردی و اجتماعی دارای نیازهای آموزشی متفاوتی هستند؛ بنابراین، بایستی برنامه‌های آموزشی متناسب با این نیازها در راستای اثربخشی بیشتر طراحی و اجرا شوند.
- آموزش‌های مرتبط با امنیت سایبری باید به‌طور مداوم به‌روز شوند تا با تغییرات فناوری و ظهور تهدیدات جدید همگام باشند.
- استفاده از روش‌های آموزشی تعاملی و جذاب، مانند بازی‌ها و شبیه‌سازی‌ها، می‌تواند اثربخشی آموزش‌ها را افزایش دهد.
- آموزش‌ها باید فراتر از ارائه اطلاعات صرف، به تقویت مهارت‌های عملی افراد بپردازند و افراد را برای مواجهه با موقعیت‌های واقعی در فضای مجازی آماده کند.
- برنامه‌ها آموزشی بایستی در کنار جنبه‌های فنی، آموزش اخلاق سایبری را در راستای تربیت شهروند دیجیتال مسئول پوشش دهند.
- آموزش‌های مرتبط با امنیت سایبری شامل مباحثی پیچیده‌ای چون شناسایی انواع کلاهبرداری‌های آنلاین، محافظت از اطلاعات شخصی، نحوه استفاده امن از شبکه‌های اجتماعی، تشخیص محتوای جعلی و غیره... است. این آموزش‌ها باید به زبانی ساده و قابل‌فهم ارائه شوند و با استفاده از مثال‌های ملموس، به مخاطبان کمک کنند تا مفاهیم را به‌درستی درک نمایند.

پیشنهادهای کاربردی

- **تاسیس رشته جرم‌شناسی سایبری:** تاسیس و توسعه یک رشته تخصصی دانشگاهی که ترکیبی از مباحث جرم‌شناسی و امنیت الکترونیک در آن تدریس گردد، می‌تواند به تربیت نیروی انسانی متخصص و آگاه به چالش‌های انسانی- فنی حوزه جرائم سایبری کمک شایانی نماید.
- **طراحی و اجرای کمپین‌های آگاهی عمومی:** ایجاد کلیشه یا کلیدواژه‌هایی چون کلیک نکن! به‌هیچ‌وجه! یا مراقب کلیک‌تان باشید و بسط گسترده آن از طریق رسانه ملی و پیام‌رسان‌ها به‌منظور ایجاد یک ذهنیت عمومی در برابر کلیک پیوندهای ناشناس می‌تواند در بالابردن سطح آگاهی سایبری عمومی موثر باشد.

- **گنجاندن آموزش امنیت سایبری در برنامه‌های درسی:** طراحی کتب درسی و کلاس‌های آموزش امنیت سایبری در چارت آموزشی مدارس و دانشگاه‌ها می‌تواند با ایجاد دانش بنیادی و تفکر انتقادی در دانش‌آموزان و دانشجویان نسبت به تهدیدات فضای سایبری، زمینه‌های رفتار مسئولانه آنلاین را در قشر جوان توسعه دهد.
- **اجرای برنامه‌های پیشگیری از جرائم سایبری:** شناسایی گروه‌های آسیب‌پذیر (کودکان، سالمندان، زنان و...) و طراحی برنامه‌های آموزشی همگانی متناسب با نیاز اقشار مختلف با بهره‌گیری از ظرفیت رسانه جمعی، سازمان‌های مردم‌نهاد و غیره... می‌تواند در کاهش شکاف دانش موجود و تقویت نقش نظارتی خانواده‌ها نقش بسزایی ایفا نماید.
- **ارایه خدمات آموزشی به بزه‌دیدگان:** راهنمایی و آگاهی‌بخشی به قربانیان جرائم سایبری در زمینه حفاظت از داده‌های شخصی، گزارش بزه‌دیدگی و شیوه‌های پیگیری حقوقی موضوع علاوه بر پیشگیری از بزه‌دیدگی مکرر، کارآمدی اقدامات پیشگیرانه کیفری و کاهش رقم سیاه جرائم را به دنبال خواهد داشت.

منابع

- ابراهیمی، سارا؛ صابری، راضیه؛ و لکی، زینب. (۱٤۰۱). نقش سواد دیجیتال و خودمراقبتی در بزه‌دیدگی در فضای مجازی. *پژوهش‌های اطلاعاتی و جنایی*، ۱۷(٦٦)، ۷۸-۵۳.
http://icra.jrl.police.ir/article_99357.html
-آرمند، محمد. (۱۳۹۰). تحلیلی بر مفهوم تعلیم و تربیت. *دوماهنامه سوره اندیشه*، (۵۲)، ٦۵-٦۲.
https://ensani.ir/file/download/article/20140611123625-9907-159.pdf
-آل‌رسول کمارعلیا، میرالتفات. (۱٤۰۱). عوامل موثر برکلاهبرداری رایانه‌ای. پایان‌نامه کارشناسی ارشد دانشگاه شهید بهشتی.
-بیگی‌راد، علیرضا؛ افشانی، سیدعلیرضا. (۱٤۰۲). ارائه مدل آموزش همگانی پلیس در افق زمانی ده‌ساله. *مطالعات فرهنگی پلیس*، *۱۰(۳)*، *۹٤-۸۱*
http://hamedan.jrl.police.ir/article_101586.html
-تدین، عباس؛ نادری، نیلوفر و عزیزی کاکوندی، محسن. (۱٤۰۲). نقش آموزش در پیشگیری از بزه‌دیدگی اطفال و نوجوانان در فضای مجازی. *پژوهش‌های جرم‌شناسی کاربردی*، ۱(۱)، ۱۱۳-۹۳.
https://www.qacr.ir/article_715537.html
-جامی پور، مونا؛ فراز پور، مهدی و اسدی، محسن. (۱۳۹۹). بررسی رابطه بین مهارت‌های سایبری و میزان بزه‌دیدگی سایبری. *پژوهش‌های اطلاعاتی و جنایی*، ۱۵(۵۹)، ۱۳٤-۱۰۷.
http://icra.jrl.police.ir/article_94729.html
-جزایری، سیدعباس؛ نعمت اللهی، میثم؛ امیریان فارسانی، امین. (۱۳۹۸). پیشگیری از جرائم سایبری و محدودیت‌های حاکم بر آن. *فصلنامه بین‌المللی قانون یار*، ۳(۱۲)، ۲٤-۹.
http://ensani.ir/file/download/article/1592112683-10125-12-1.pdf
-جلالی فراهانی، امیرحسین؛ باقری اصل، رضا. (۱۳۸٦). پیشگیری اجتماعی از جرائم و انحرافات سایبری. *مجلس و پژوهش*، ۱٤(۵۵)، ۱۵٦-۱۲۲.
https://rc.majlis.ir/fa/book_pub/show/837544
-چاوشی، محمد صادق؛ کرامتی معز، هادی. (۱۳۹۷). عوامل و آثار بزه‌دیدگی اخلاقی کودکان و نوجوانان در شبکه اجتماعی تلگرام و اینستاگرام. *پژوهش‌های اخلاقی*، ۹(۲)، ۱۲۲-۱۰۵.
http://akhlagh.saminatech.ir/Article/17333/FullText
-حسنی، جعفر. (۱۳۸۸). *معیارهای جرم‌انگاری موارد نقض حریم داده‌های شخصی در فضای سایبر، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات*. چاپ اول. انتشارات روزنامه رسمی کشور.
-خمسه‌ای، علی محمد. (۱۳۸۲). تأثیر آگاه‌سازی اجتماعی ناجا بر نگرش دانش‌آموزان نسبت به پلیس و انحرافات اجتماعی. پایان‌نامه کارشناسی ارشد دانشکده فرماندهی و ستاد دانشگاه علوم انتظامی.
-درویشی، صیاد؛ اسداللهی، بهروز؛ میرزاخانی، دکترعبدالرحمان و رشنودی، بهروز. (۱٤۰۳). بررسی رابطه فرهنگ ایرانی و اسلامی در پیشگیری از آسیب‌های اجتماعی جهانی‌شدن ارتباطات و اطلاعات. *مطالعات فرهنگی پلیس*، ۱۱(۱)، ۳۳-٤۱.
http://hamedan.jrl.police.ir/article_102507.html

-رجبی، ابراهیم. (۱۳۸۹). درمانگاه بزه‌دیده و بزه‌دیدگی و نقش پلیس در آن. *دانش انتظامی*، ۱۲(۱)، ۷-۳۳.

http://pok.jrl.police.ir/article_97027.html

-رضوی فرد، بهزاد؛ رباط جزی، محمدتقی؛ عمرانی، گلسا. (۱۳۹۷). پیشگیری از بزه‌دیدگی جنسی در شبکه‌های اجتماعی. *حقوقی دادگستری، ۸۲(۱۰٤)، ٦٥-۳۹.*

https://www.jlj.ir/article_34676.html

-رضوی، محمد. (۱۳۸٦). جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آنها. *دانش انتظامی*، ۹(۱)، ۱٤۰-۱۲۰.

http://pok.jrl.police.ir/article_97368.html

-زیبر، اولریش. (۱۳۸۳). *جرائم رایانه‌ای*، ترجمه محمد علی نوری، چاپ اول. انتشارات گنج دانش.

-سلیمی‌قلعه، احسان. (۱٤۰۱). سیاست جنایی مشارکتی در فضای سایبر؛ از ضرورت و کارایی تا تدابیر اجرایی. *جامعه فرهنگ رسانه، ۱۱(٤۳)، ۲۹۲-۲۷۳.*

https://www.jscm.ir/article_156025.html

-سیدین بروجنی، زهره؛ موذن، فرانک؛ بهشتی، اکرم. (۱٤۰۲). پیشگیری غیرکیفری از بزه‌دیدگی زنان در فضای سایبری. *مطالعات پیشگیری از جرم، ۱۸ (٦۷)، ۱۷-۱.*

http://cps.jrl.police.ir/article_99900.html

-صادقی رام، رقیه؛ موذنی، روح الله؛ پوررشید، سیده زهرا. (۱٤۰۰). مطالعه‌ی تطبیقی همگانی‌بودن و آزادی آموزش در قانون اساسی ایران و اسناد بین‌المللی، با تاکید بر راهکارهای حل تعارض. *پژوهشنامه حقوق تطبیقی*، ۵(۲)، ۱۷۹-۱٦۱.

https://lps.journals.umz.ac.ir/article_3491.html

-صادقی، محمود (۱۳۹۹). افزایش ۱۰۰ درصدی مصرف اینترنت در کشور با شیوع ویروس کرونا. *مرکز پژوهش‌های مجلس شورای اسلامی.*

https://rc.majlis.ir/fa/news/show/1509627

-صبح خیز، رضا؛ پورقهرمانی، بابک؛ صفاری، علی. (۱۳۹۹). الگوی راهبردی مقابله با جرائم سایبری در ایران. *فصلنامه مطالعات راهبردی ناجا*. ۵(۱۸)، ۱۱۲-۷۷.

http://ssj.jrl.police.ir/article_95711.html

-صیادی تورانلو، حسین؛ میرغفوری، سیدحبیب‌اله؛ مهدوی، محمدرضا؛ ثقفی، سپیده. (۱۳۹۹). تحلیل عوامل مرتبط بر ایجاد جرائم فضای مجازی با استفاده از رویکرد فازی. *پژوهشنامه نظم و امنیت انتظامی*، ۱۳(۳)، ٥٤-۲۷.

http://osra.jrl.police.ir/article_94388.html

-فرهادی آلاشتی، زهرا. (۱۳۹٥). *پیشگیری وضعی از جرائم سایبری: راهکارها و چالش‌ها*. چاپ اول. بنیاد حقوقی میزان.

-قاسمی پیربلوطی، اکبر؛ عزیزمراد، مرادی. (۱۳۹۸). تعامل پیشگیرانه پلیس و مدارس؛ زمینه‌های ایجاب، راهکارهای تحقق. *آموزش در علوم انتظامی*، ۷(۲٦)، ۲۱۲-۱٦۹.

http://tps.jrl.police.ir/article_93243.html

-کرد علیوند، روح الله؛ میرزایی، محمد. (۱۳۹۷).گونه‌شناسی جرائم سایبری با نگاهی به قانون جرائم رایانه‌ای و آمار پلیس فتا. *حقوقی دادگستری*،۸۲ (۱۰۲)، ۲۰۷-۱۹۱.
https://www.jlj.ir/article_32738.html
-گرکی، مارکو. (۱۳۸۹). *جرائم سایبری راهنمایی برای کشورهای در حال توسعه*. ترجمه مرتضی اکبری. تهران: پلیس فتا.
-محمودی، مرضیه. (۱٤۰۰). علل مؤثر بر وقوع بزه‌دیدگی کلاهبرداری رایانه‌ای: با مطالعه‌ی میدانی پرونده‌های سوءاستفاده از ای‌تی‌ام تهران ۱۳۹۷ – ۱۳۹۵، *چهارمین کنگره بین‌المللی تحقیقات بین‌رشته‌ای در علوم انسانی اسلامی، فقه، حقوق و روانشناسی*.
https://www.symposia.ir/HUMANITY04
-مرشدی، مسعود؛ آل‌رسول کمارعلیا، میرالتفات. (۱٤۰۲). بررسی رفتارهای بزه‌دیده‌ساز قربانیان کلاهبرداری اینترنتی در پرتو روانشناسی جنایی. *پژوهشنامه نظم و امنیت انتظامی، ۱٦(۲)، ۷۰-۲۷*.
http://osra.jrl.police.ir/article_101325.html
-مرندی، الهه؛ قربانی، اعظم. (۱٤۰۰). مبانی و سازوکارهای حمایتی حق آموزش در قانون اساسی جمهوری اسلامی ایران و اسناد حقوق بشری. *مطالعات حقوق بشر اسلامی*، ۱۰(۲۰)، ۱۰۲-۷۹.
https://www.pfbaj.ir/article_128555.html
-میر، فاطمه. (۱۳۹٤). نقش بزه‌دیده در تحقق جرائم سایبری. پایان‌نامه کارشناسی ارشد دانشگاه فردوسی.
-نیازپور، امیرحسین. (۱۳۸۵). اقدامات دستگاههای دولتی ایران در زمینه پیشگیری از بزهکاری. *آموزه‌های حقوق کیفری*، ۳(۲۰)، ۸۸-٦۱.
https://cld.razavi.ac.ir/article_1353.html

- Abdullah, A. T. & Jahan, I. (2020). Challenges of Cyber Policing in Response of Cybercrime to Reduce Victimization. *International Journal of Research and Innovation in Social Science*, 4(5), 219-226.
https://api.semanticscholar.org/CorpusID:219707329
-Agustina, J. A. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology*, 9 (1), 35-54.
https://doi.org/10.5281/zenodo.22239
-Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE, *International Journal of Information Technology and Language Studies (IJITLS)*. 3(2), 8-29.
http://journals.sfu.ca/ijitls
-CIORBARU, A. N. (2018). Crime Prevention Through Education, Law, Society & Organisations, *Romanian Foundation for Business Intelligence*, Editorial Department, 3(5), 75-79.
https://seaopenresearch.eu/Journals/articles/LSO_5_2.pdf
-Corradini, I., Nardelli, E. (2020). *Social Engineering and the Value of Data: The Need of Specific Awareness Programs*. In: Ahram, T., Karwowski, W. (Eds) Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960. Springer, Cham. pp. 59-65,
https://doi.org/10.1007/978-3-030-20488-4_6

-Crews, G. (2009). *Education and crime. In J. M. Miller 21st Century criminology: A reference handbook* (pp. 59-66). SAGE Publications, Inc.,
https://www.doi.org/10.4135/9781412971997.n8
-Daniela, L. & Rudolfa, A. (2018). The Role of Parents for Developing Digital Literacy of 0-5 Year Olds. In L. Daniela & M. Lytras (Eds.), *Learning Strategies and Constructionism in Modern Education Settings* (pp. 104-113). IGI Global.
https://doi.org/10.4018/978-1-5225-5430-1.ch007
-De, R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55(102171), 1-5.
https://doi.org/10.1016/j.ijinfomgt.2020. 102171
-Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17-33.
https://doi.org/10.1108/JCRPP-12-2019-0070
-Habirovs, A. (2018). Factors that shape cybercrime victimisation and use of prevention measures in England and Wales. *Masters thesis*, University of Huddersfield.
https://core.ac.uk/download/228132905.pdf
-Halder, D. (2022). *Cyber victimology: decoding cyber-crime victimisation*, Routledge, New York.
https://doi.org/10.4324/9781315155685
-Holt, T.J. **&** Bossler, A.M. (2014). *An assessment of the current state of cybercrime scholarship*, Deviant Behavior, 35(1), 20-40.
https://doi.org/10.1080/01639625.2013.822209
-Iceberg Cyber Security (2023). Critical Thinking & Cyber Security.
https://www.linkedin.com/pulse/critical-thinking-cyber-security-iceberg-cyber-security-/
-Jamil, H. (2022). *Factors Affecting Users Cybersecurity Practices: A Study of Australian Microbusinesses*, Submitted to Charles Sturt University in fulfilment of the requirements for the Doctor of Philosophy at Charles Sturt University, Charles Sturt University: Australia.
https://researchoutput.csu.edu.au/en/publications/factors-affecting-users-cybersecurity-practices-a-study-of-austra
-Joshi, S.V., & Deshpand, P.K. (2022). *Cyber Crime Education*, 11(1), 97-98.
https://doi.org/10.53957/sanshodhan/2022/v11i1/169805
-Karagiannopoulos, V., Kirby, A. L., Oftadeh Moghadam, S., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: a Portsmouth case study. *Computer Law & Security Review*, 43 (105615). 1-9.
https://doi.org/10.1016/j.clsr.2021.105615
-Kurylo, V., Karaman, O., Bader, S., & Pochinkova, M., Stepanenko, V. (2023). Critical thinking as an information security factor in the modern world. *Social Legal Studios*. 6(3), 67-74.
https://doi.org/10.32518/sals3.2023.67
-Leukfeldt, E. R. (2017). *Research agenda the human factor in cybercrime and cybersecurity. Netherlands: Eleven international publishing***.**
https://securitydelta.nl/media/com_hsd/report/141/document/Research-Agenda-The-Human-Factor-in-Cybercrime-and-Cybersecurity.pdf
-Mehrparsa, S. (2022). The Effect of Digital Literacy and Parental Mediation on the Risks of Online Education about the Mediating Role of Students' Self-Control, *Technology and Scholarship in Education*, 1(2), 35-44.
https://journals.pnu.ac.ir/article_8718.html

-Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: stakeholder perspectives. *BMC public health*, 13(543), 1-6.
https://doi.org/10.1186/1471-2458-13-543
-Morgan, S. (2020). *cybercrime to cost the world $10.5 trillion annually by 2025*, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
-Santhosh, T. & Thiyagu, K. (2024). Fostering responsible behavior online-relevance of cyber ethics education. *Malaysian Online Journal of Educational Technology*, 12(1), 32-38.
http://dx.doi.org/10.52380/mojet.2024.12.1.428
-Sarker, O., Jayatilaka, A., Haggag, S., Liu, C. & Babar, M.A. (2024). A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness, *Journal of Systems and Software*, 208(111899), 1-25.
https://doi.org/10.1016/j.jss.2023.111899
-Shillair, R., Cotten, S.R., Tsai, H.Y.S., Alhabash, S., LaRose, R. & Rifon, N.J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.
https://doi.org/10.1016/j.chb.2015.01.046.
-Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection *Behavior, PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS (PACIS)* 2015 Proceedings. 31.
http://aisel.aisnet.org/pacis2015/31
-Ssenyonjo, M. (2009). *Economic, Social and Cultural Rights in International Law*, Hart Publishing.
https://doi.org/10.4324/9781315257044.
-Statista (2019), *"Number of internet and social media users worldwide as of October 2023"*, available at:
www.statista.com/statistics/617136/digitalpopulation-worldwide/
-Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & behavior*. 7(3), 321-326.
http://dx.doi.org/10.1089/1094931041291295
-UNESCO Institute for Statistics. (2018). *A Global Framework of Reference on Digital Literacy Skills for Indicator* 4.4.2,
https://unesdoc.unesco.org/ark:/48223/pf0000265403.locale=en
-Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, 19(1), 39-53.
https://doi.org/10.1177/1461355716681810
-Zeniali Khorchani, S., Rezaei, S., Saadatmand, Z., & Farashbandi, R. (2019). The Effectiveness of Creative Thinking Training on the Critical Thinking and Media Literacy in Students. *IEEPJ*. 1(3), 213-221.
http://ieepj.hormozgan.ac.ir/article-1-95-en.html
-Zur, O. & Zur, A. (2011). *On Digital Immigrants and Digital Natives: How the Digital Divide Affects Families, Educational Institutions, and the Workplace*. Zur Institute - Online Publication.
http://www.zurinstitute.com/digital_divide.html