



نقش و جایگاه سواد حریم خصوصی بر خط در حفاظت از اطلاعات شخصی

صالح رحیمی^۱، وکیل احمدی^۲، زهره عزیزی^۳

DOR: 20.1001.1.17358671.1399.19.69.4.3

چکیده:

هدف از این پژوهش، بررسی سواد حریم خصوصی برخط به عنوان راهکاری برای حمایت از حریم خصوصی برخط است. این مقاله از لحاظ هدف کاربردی و با روش اسنادی و به شیوه توصیفی انجام شده است؛ بنابراین ضمن بررسی نگرانی‌های حریم خصوصی افراد در اینترنت و تناقض حریم خصوصی، به سواد حریم خصوصی برخط و ابعاد آن پرداخته می‌شود و در ادامه تهدیدات حریم خصوصی و راهکارهایی حفظ از آن و همچنین راه رسیدن به سواد حریم خصوصی برخط عنوان شده و در نهایت، پیشنهادهایی برای افزایش این سواد ارائه می‌گردد.

یافته‌ها حاکی از آن است که سواد حریم خصوصی برخط به عنوان دانشی برای حفاظت از اطلاعات شخصی، سواد ضروری برای زندگی در عصر دیجیتال است که با فراهم کردن آگاهی از مسائل مربوط به حریم خصوصی برخط از قبیل آگاهی از تهدیدات و خطرات حریم خصوصی برخط و همچنین آگاهی از راهکارهای لازم برای کنترل حریم خصوصی برخط، کاربران را در حفظ اطلاعاتشان یاری می‌رساند. با توجه به اهمیت افزایش سواد حریم خصوصی برخط در جهت حفظ حریم خصوصی در اینترنت، باید آموزش و اقدامات لازم در جهت ارتقاء سواد حریم خصوصی برخط افراد صورت گیرد.

کلیدواژه‌ها: سواد حریم خصوصی برخط، تناقض حریم خصوصی برخط، تهدیدات حریم خصوصی برخط، راهکارهای حفظ حریم خصوصی برخط، اینترنت.

۱-s.rahimi@razi.ac.ir
۲-v.ahmadi@razi.ac.ir
۳-z.azizi.1396@gmail.com

۱. استادیار گروه علم اطلاعات و دانش‌شناسی، دانشگاه رازی (نویسنده مسئول)
۲. استادیار گروه جامعه‌شناسی، دانشگاه رازی
۳. کارشناس ارشد علم اطلاعات و دانش‌شناسی، دانشگاه رازی

مقدمه و بیان مسئله:

امروزه پیشرفت فناوری اطلاعات و فضای مجازی و توسعه یافتن شرکت‌های تجاری و غیرتجاری و افزایش نیاز حکومت‌ها به جمع‌آوری مقداری از اطلاعات از جمله داده‌های شخصی افراد برای ارائه خدمات، حمایت امنیت ملی و مبارزه با جرائم و غیره، سبب شده که داده‌های شخصی افراد با خطرات بزرگ و متعدد روبه‌رو شوند (عتقی، ۱۳۹۷: پ).

افراد در طول روز مدام در حال ارائه اطلاعات خصوصی خود به کسانی هستند که آن‌ها در مقابل هیچ تعهدی برای ارائه اطلاعات شفاف از خود ندارند. افراد جامعه دائماً در حال خودافشایی به حکومت‌ها هستند. حکومت‌های امروز دنیا خیلی راحت می‌توانند به بهانه ارائه خدمات به اطلاعات خصوصی ما دسترسی داشته باشند. آن‌ها می‌توانند از طریق برنامه‌هایی که خودشان تعیین می‌کنند حریم خصوصی افراد را نقض کنند. برای مثال مدیر پیشین بخش اطلاعاتی جامعه یونسکو در حمایت از حریم خصوصی نکاتی تکان‌دهنده را گوشزد کرده است. او می‌گوید ایالات متحده آمریکا با همکاری انگلستان، کانادا، استرالیا و نیوزلند از شبکه‌های اجتماعی که در اختیار دارند برای شنود، کنترل و پردازش اطلاعات روزانه بیش از سه میلیارد پیام تلفنی، دورنگار و پست الکترونیکی در سراسر دنیا استفاده می‌کنند و هرگونه حرکت و فعالیت افراد در خانه و محل کار و مکان فراغت و مانند آن را کنترل می‌کنند (شهیری، ۱۳۸۶: ۱۲۸). علاوه بر این شرکت‌های تجاری فعال در زمینه‌های جمع‌آوری و پردازش اطلاعات نیز می‌کوشند به شیوه‌های مجاز و غیر مجاز این اطلاعات را گردآوری کنند و به مؤسسات خواستار آن‌ها بفروشند (معمذنژاد، ۱۳۸۴؛ نقل از خوش‌رفتار و محمدپور، ۱۳۹۶: ۳).

شبکه‌های اجتماعی با استفاده از اطلاعات زیادی که هنگام ثبت‌نام از افراد درخواست می‌کنند و یا با رصد کردن رفتار افراد در شبکه و افزودن این اطلاعات به بانک داده‌های خود، مجموعه‌ای از اطلاعات را جمع‌آوری کرده و از طریق داده‌کاوی، پروفایل‌های شخصی برای اعضا می‌سازند که حاوی اطلاعات بسیار زیادی از زندگی خصوصی افراد است و به این ترتیب به حریم خصوصی تعداد بیشتری از مردم جهان وارد می‌شوند. کافی است این اطلاعات دسته‌بندی شده و در کنار هم قرار گیرند و به این ترتیب می‌توان یک پروفایل کامل از شخصیت هر فرد ایجاد کرد که در آن نقاط قوت و ضعف، علایق سیاسی، اعتقادی، اخلاقی وی مشخص شده باشد. (حبیبی، ۱۳۹۵: ۳۹). وجود چنین اطلاعاتی در محیط مجازی بسیاری از افراد را که به دنبال ارتکاب جرم به انگیزه‌های مختلف هستند، وسوسه می‌کند تا از این محیط استفاده کنند.

امروزه اینترنت، تجاوزه و تعدی به حریم خصوصی اشخاص را که از بنیادی‌ترین و اساسی‌ترین حقوق بشری تلقی می‌شود و با شخصیت وی ارتباط تنگاتنگ دارد، بیش از پیش سهل‌الوصول کرده است؛ به گونه‌ای

که مجرمان در اقصا نقاط جهان فارغ از مرزهای جغرافیایی، اطلاعات افراد را مورد تعرض قرار می‌دهند. اگر پیش از ظهور اینترنت توانایی ورود به حریم خصوصی اشخاص و سرقت اطلاعات محدود بود، با ظهور آن امکان طرح‌ریزی و هتک حریم خصوصی و سرقت اطلاعات سری و خصوصی اشخاص فراهم گشت که پیش از آن تصورش هم نمی‌رفت (فتحی و شاهمادی، ۱۳۹۶: ۲۳۵).

بنابراین، یکی از نگرانی‌های اساسی دربارهٔ برخاسته بودن کاربران اینترنت، حفظ حریم خصوصی‌شان است. برای هر فرد ممکن است اطلاعات خاصی حریم خصوصی او حساب شود که اگر از طریق اینترنت یا هر روش دیگری فاش شود، ضررهای هنگفتی به شخصیت، موقعیت، مال یا آبروی او وارد شود. اطلاعاتی مانند مسائل خانوادگی یا مالی یا پزشکی از این نوع اطلاعات است.

یکی از جدی‌ترین دلایلی که سبب شیوع جرائم نقض حریم خصوصی در فضای اینترنت شده است، فقدان آگاهی در خصوص رویه‌های حفظ حریم خصوصی و امنیت در میان کاربران این فناوری است. چراکه همواره افراد سودجویی وجود دارند که از آب گل‌آلود ماهی بگیرند و با سرقت اطلاعات شخصی، افراد ناآگاه را مورد سوءاستفاده قرار دهند.

اما متأسفانه تاکنون قوانین کاملی در زمینه پردازش و استفاده از داده‌های شخصی افراد و مجازات‌های برای ناقضان وجود نداشته است و در خیلی از مواقع قوانین نمی‌تواند بسیاری از خسارت‌های که برای افراد به بار آمده را جبران کند. وقتی قانونی نتواند در صورت نقض حریم خصوصی از کاربر حمایت کند و یا قوانین سلبی و بازدارنده برای حفظ تمامیت حریم شخصی کاربر فضای مجازی نداشته باشد، این خود کاربر است که وظیفه حفظ حریم شخصی خود را به شکلی پیشگیرانه به عهده می‌گیرد.

لذا، اتخاذ راهکارهای پیشگیرانه مؤثر و روزآمد در این راستا از مهم‌ترین پیش‌نیازهای حفاظت از حریم خصوصی در عصر دیجیتال است و اگرچه فناوری اطلاعات، معمولاً یکی از عمده‌ترین دلایل نقض حریم خصوصی تلقی می‌گردد، راه‌های گوناگونی نیز وجود دارد که از طریق آن‌ها این فناوری، خود قادر به حمایت از محرمانگی و پیشگیری از نقض آن می‌باشد. امروزه رهنمودها و شیوه‌های محافظت از حریم خصوصی که به روش‌های علمی طراحی شده‌اند، مورد استفاده قرار می‌گیرند. این امکانات، طیف وسیعی از تمهیدات و راهکارها از روش شناسایی‌های طراحی‌شده بر مبنای اطلاع‌رسانی اخلاقی تا رمزنگاری به‌منظور محافظت از اطلاعات شخصی در مقابل استفاده غیرمجاز را در برمی‌گیرد (محسنی و صوفی زمر، ۱۳۹۶: ۹۳).

نبود سواد لازم برای استفاده صحیح از این فضای پیش رو و از طرف دیگر ضعف آموزش‌های لازم به افراد جامعه، موجب گردیده است که استفاده از اینترنت به خطری برای نقض حریم خصوصی منجر شود؛ اما افراد باوجود تمایل برای حفاظت از حریم خصوصی، توانایی و مهارت لازم را در این زمینه

ندارند. مطالعات (پاین^۱ و دیگران، ۲۰۰۷؛ ویلس و زلکوویچ^۲، ۲۰۱۱) نشان دادند که کاربران نگران حفظ حریم خصوصی شان در اینترنت بوده و مایل به حفاظت از آن هستند؛ اما تحقیقاتی نیز نشان می‌دهد کاربران باوجود داشتن این نگرانی، داوطلبانه اطلاعات شخصی خود را در اینترنت افشا می‌کنند (اکویستی و گراس^۳، ۲۰۰۶؛ برونستاین^۴، ۲۰۱۴؛ دباتین^۵ و دیگران، ۲۰۰۹؛ توفکسی^۶، ۲۰۰۸؛ ژیتمیرسکی - جفت و براتسپیس^۷، ۲۰۱۴)، پژوهشگران یکی از دلایل این تناقض را نبود سواد حریم خصوصی برخط^۸ کاربران می‌دانند (Quoted from Weinberger, Bouhnik & Zhitomirsky-Geffet, 2017: 4).

سواد حریم خصوصی برخط به‌عنوان دانشی برای حفاظت از اطلاعات شخصی، سواد ضروری برای زندگی در عصر دیجیتال است که با فراهم کردن دانش در مورد آگاهی از شیوه سازمان‌ها، مؤسسات و ارائه‌دهندگان خدمات برخط^۹، آگاهی از جنبه‌های فنی حریم خصوصی برخط و حفاظت از داده‌ها^{۱۰}، آگاهی از قوانین و جنبه‌های قانونی حفاظت از داده‌های برخط^{۱۱}، آگاهی از دستورالعمل‌ها در مورد حریم خصوصی و حفاظت از داده‌ها^{۱۲} و آگاهی از راهکارهای لازم برای کنترل حریم خصوصی فردی^{۱۳}، کاربران را در حفظ اطلاعاتشان یاری می‌رساند (Trepte et al. 2015: 2). این سواد مهارتی است که لازم است کاربران در کنار استفاده از اینترنت به‌عنوان یک رسانه تعاملی به آن مجهز شوند. چراکه استفاده از اینترنت بدون داشتن سواد حریم خصوصی برخط، می‌تواند با اثرات نامطلوبی همراه باشد. بدین لحاظ لازم است که کاربران نسبت به کسب این سواد در همه ابعاد آن اقدام کنند و از آسیب‌ها و زیان‌های ناشی از عدم کسب سواد حریم خصوصی برخط در امان باشند.

مرور پژوهش‌های مربوط به حریم خصوصی برخط در خارج از کشور نشان می‌دهد، پژوهشگران تحقیقات متعددی را پیرامون این موضوع نظیر رفتارهای حفاظت از حریم خصوصی، نگرانی‌های حریم خصوصی، انگیزه‌های حفاظت از حریم خصوصی برخط و غیره انجام داده‌اند ولی تنها تعداد انگشت‌شماری به سواد حریم خصوصی برخط پرداخته‌اند که در ادامه به آن‌ها اشاره می‌شود.

یون^{۱۴} (۲۰۰۹) با استفاده از نظریه انگیزه محافظت راجرز، عوامل تعیین‌کننده نگرانی‌های مربوط به حفظ حریم خصوصی را که بر رفتار حفظ حریم خصوصی اثر می‌گذارد، شناسایی کرد. او بیان کرد

1. Paine
2. Wills & Zeljkovic
3. Acquišiti & Gross
4. Bronštein
5. Debatin
6. Tufekci
7. Zhitomirsky-Geffet & Bratspiess
8. Online Privacy Literacy (OPL)
9. Knowledge about practices of organizations, institutions and online services providers
10. Knowledge about technical aspects of online privacy and data protection
11. Knowledge about laws and legal aspects of online data protection
12. Knowledge about directives on privacy and data protection
13. Knowledge about user strategies for individual privacy regulation
14. Youn

که درک خطرات افشای اطلاعات، باعث افزایش و مزایای درک شده توسط مبادله اطلاعات، باعث کاهش نگرانی‌های امنیتی می‌شود.

روتمن^۱ (۲۰۰۹) چارچوبی را برای سواد حریم خصوصی در زمینه رسانه‌های اجتماعی ارائه کرد که شامل پنج مؤلفه بود: درک جنبه‌های مختلف اطلاعات شخصی، شناخت تعاملات اجتماعی برخط به‌عنوان یک مکان برای تهدیدات بالقوه حریم خصوصی، درک نتایج احتمالی انتشار اطلاعات در تعاملات اجتماعی برخط، ارزیابی خطرات و مزایای به اشتراک گذاری اطلاعات شخصی، تصمیم‌گیری در مورد زمان و چگونگی به اشتراک گذاری اطلاعات شخصی.

ویجس^۲ و دیگران (۲۰۱۲) در پژوهشی مفهومی را با عنوان سواد حریم شخصی، به‌منظور توضیح نگرش مصرف‌کنندگان در مورد پردازش اطلاعات شخصی ارائه دادند و شاخص سواد حریم خصوصی را تعیین کردند.

پارک (۲۰۱۳) در مقاله‌ای تأثیر سه بعد سواد دیجیتال (آشنایی با جنبه‌های فنی اینترنت، آگاهی از شیوه‌های نظارت سازمان‌ها و درک سیاست‌های حفظ حریم) را در ارتباط با رفتارهای حریم خصوصی برخط بررسی کرد و نشان داد که دانش سواد دیجیتال کاربر، قدرت زیادی برای پیش‌بینی رفتار کنترل حریم خصوصی دارد.

تریت و دیگران (۲۰۱۵) از طریق تحلیل منابع، مقیاسی را برای سواد حریم خصوصی برخط با پنج بعد (آگاهی از شیوه ارائه‌دهندگان خدمات برخط، آگاهی از جنبه‌های فنی حریم خصوصی برخط، آگاهی از قوانین حفاظت از اطلاعات، آگاهی از دستورالعمل‌های حفاظت از اطلاعات و آگاهی از راهکارهای لازم برای کنترل فردی) مطرح کردند.

بارتس و دینلن^۳ (۲۰۱۶) بیان می‌کنند که افرادی که وقت بیشتری را در فیس‌بوک صرف می‌کنند و کسانی که در تغییر تنظیمات حریم خصوصی تجربه بیشتری دارند، سواد حریم خصوصی برخط بیشتری نیز دارند و همچنین، سواد حریم خصوصی برخط باعث افزایش رفتار حفاظت حریم خصوصی می‌شود. نتایج پژوهش وینبرگر، ژیتمیرسکی - جفت و بوهنیک (۲۰۱۷) نشان داد که عوامل انگیزشی مانند نگرانی کاربران از حفظ حریم خصوصی و حس ناشناس بودن هنگام بازدید از وب‌سایت، قوی‌ترین عوامل پیش‌بینی‌کننده سطح سواد حریم خصوصی برخط کاربران هستند.

وینبرگر، بوهنیک و ژیتمیرسکی - جفت (۲۰۱۷) بیان می‌کنند که کاربران با سطح بالایی از نگرانی از حریم خصوصی برخط و خودکارآمدی در حفظ حریم خصوصی، رفتار حفاظت از حریم خصوصی بیشتری دارند.

1. Rotman

2. Veghes

3. Bartsch & Dienlin

ماکلی^۱ (۲۰۱۸) چالش‌های کتابخانه‌های عمومی برای حمایت از فناوری‌های حفاظت از حریم خصوصی را عدم آگاهی کاربران، کتابداران و کارکنان کتابخانه با ابزارهای فناوری، نیاز به پشتیبانی تعداد زیادی از ابزارها و فناوری و همچنین نبود درکی درست از دیدگاه سازندگان اصلی ابزارها، مطرح کرد.

با توجه به اینکه اکثر پژوهش‌های مربوط به سواد حریم خصوصی برخاسته از چند سال اخیر انجام شده است، در داخل کشور تنها مطالعه‌ای که در زمینه سواد حریم خصوصی یافت شد، مربوط به مقاله سیاسی‌راد و بیچرانلو (۱۳۹۶) است که ضمن بررسی تناقض حریم خصوصی، مزایا و خطرهای خودافشاگری را مطرح کرده و بر اساس سواد حریم خصوصی برخاسته، برخی از راهبردهای اجتماعی و فناوری را برای حل تناقض حریم خصوصی معرفی کرده است.

لذا، با توجه به نگرانی‌های نقض حریم خصوصی برخاسته، اهمیت افزایش سواد در جهت حفظ حریم خصوصی افراد در اینترنت بیشتر می‌شود و از آنجاکه جامعه ما نیز باید خود را با تهدیدهای فضای اینترنت همگام سازد و از طرف دیگر تابه‌حال پژوهشی در جامعه ما جهت ضرورت و تفهیم سواد حریم خصوصی برخاسته کمتر مورد توجه بوده، نیاز به بررسی آن ضروری است. از طرفی دیگر شناخت و توجه به این سواد منجر به برنامه‌ریزی دقیق‌تر و تدارک هدفمند امکانات مورد نیاز آموزشی و آگاهی‌رسانی برای شهروندان می‌شود و می‌تواند به پیشبرد اهداف پیشرفت و امنیت کشور در عصر دیجیتال کمک کند.

حریم خصوصی در اینترنت

ارائه تعریف دقیق و کامل برای حریم خصوصی کار دشواری است، زیرا عناصری نظیر عرف و فرهنگ اجتماعی و زمان و روحیات افراد در تعیین آن مؤثرند و به لحاظ متفاوت بودن این‌گونه عوامل در کشورهای گوناگون و نیز نسبت به اشخاص مختلف، تعیین معیارهای مشخص و تعریف جامع برای آن امری دشوار است (محسنی و قاسم‌زاده، ۱۳۸۵: ۲)؛ اما به‌طورکلی آنچه که از تعاریف حریم خصوصی که صاحب‌نظران ارائه کرده‌اند می‌توان استنباط کرد، این است که حریم خصوصی، حق افراد در مورد تصمیم‌گیری در مورد اطلاعات شخصی‌شان است و این حق هرگونه مداخله دیگران را در زندگی خصوصی آن‌ها سلب می‌کند. افراد اجتماع هر یک اطلاعاتی دارند که با میل به مخفی نگه‌داشتن آن‌ها، نمی‌خواهند که سایرین نسبت به آن علم و آگاهی پیدا کنند. این دسته از اطلاعات، آنگاه که به حیطه خصوصی فرد مربوط باشد، حریم خصوصی وی به شمار می‌آید و آنگاه که به نحوی در اینترنت نشر پیدا می‌کند، صحبت از حریم خصوصی افراد در اینترنت به میان می‌آید.

گسترش و زیاد شدن شرکت‌های تجاری و وسعت فعالیت و خدمات‌شان، توسعه یافتن شبکه‌های اجتماعی، دولت الکترونیک و خدمات الکترونیک دیگر در اینترنت، باعث می‌شود که هر فردی مجبور

به دادن داده‌های شخصی خود در محیط اینترنت باشد که به‌منظور تسهیل امور در رابطه با زندگی روزمره و پاسخگویی سریع به نیازها است. اطلاعات گوناگونی که درباره اشخاص در اینترنت قرار داده می‌شود، امکان نقض حریم خصوصی افراد را به‌شدت افزایش می‌دهد و بسیاری از افراد را که به دنبال ارتکاب جرم به انگیزه‌های مختلف هستند، وسوسه می‌کند تا از این محیط استفاده کنند؛ بنابراین، برخط بودن کاربران اینترنت، به یکی از نگرانی‌های اساسی در مورد حریم خصوصی افراد تبدیل شده است. به‌طوری‌که اینترنت از سوی اشخاص سودجو به گونه‌ای مورد استفاده قرار می‌گیرد که به بزرگ‌ترین نقض‌کننده حریم خصوصی افراد تبدیل شده است و با افزایش این نگرانی‌ها، ارسال اطلاعات ناقص افزایش یافته و همچنین شکایت‌های مربوط به جرائم اینترنتی مربوط به نقض حریم خصوصی افراد افزایش می‌یابد؛ بنابراین ضروری است که افراد برای رفع این مشکلات اقدام کنند و با ایجاد سازوکارهای امنیتی و راهکارهای دیگر، شرایطی را ایجاد نمایند که اطمینان کنند که حریم خصوصی‌شان حفظ می‌شود.

سواد حریم خصوصی راه حلی برای رفع تناقض حریم خصوصی برخط بنا بر نظریه آگاهی^۱ آلتمن^۲ در هر مرحله از رشد روابط میان افراد نیروهای متناقضی وجود دارد که از یک‌سو موجب حفظ حریم خصوصی و فاصله از دیگران می‌شود و از سوی دیگر فرد را به سمت خودافشاکری می‌کشاند (درلگا^۳ و دیگران، ۲۰۰۸؛ نقل از سیاسی‌راد و بیچرانلو، ۱۳۹۶: ۱۲۶). درنتیجه این تناقض که با عنوان (تناقض حریم خصوصی) شناخته می‌شود، کاربران ممکن است باوجود اطمینان از تهدید، برای حفظ حریم خصوصی خود اقدامی نکنند. این تناقض که با عنوان دوگانه نگرش یا رفتار نیز شناخته می‌شود، در محیط اینترنت بدین معناست: کاربر باوجود نگرانی فراوان در مورد حریم خصوصی خود (نگرش) همچنان به گونه‌ای فعال اطلاعات خود را در اینترنت به اشتراک می‌گذارد (رفتار) (لی^۴ و دیگران، ۲۰۱۳؛ نقل از سیاسی‌راد و بیچرانلو، ۱۳۹۶: ۱۲۶). تریپت و دیگران (۲۰۱۵: ۷) بیان داشتند که محققان چهار فرضیه را برای توجیه، تناقض حریم خصوصی برخط بیان کردند که عبارتند از:

۱- فرضیه رضایتمندی^۵ به این صورت تعریف می‌شود که کاربران مزایا و خطرات کار را بررسی می‌کنند و سپس با مقایسه مزایای نتایج رسیدن به هدف و خطرات ممکن، با رضایتمندی در این خصوص تصمیم می‌گیرند که آیا اطلاعات خود را در اختیار دیگران قرار دهند یا نه.

۲- فرضیه تعصب خوش‌بینانه^۶ که به آن خوش‌بینی غیرواقعی نیز گفته می‌شود به‌عنوان یک توضیح برای افشای اطلاعات شخصی کاربران در نظر گرفته شده است. افراد در این حالت فکر می‌کنند که نسبت

1. Privacy Regulation Theory

2. Altman

3. Derlega

4. Lee

5. Gratification hypothesis

6. Measurement bias hypothesis

به دیگران آسیب پذیری کمتری دارند و خطرات ممکن را، بیشتر متوجه افراد دیگر می‌دانند. این حالت معمولاً در هنگام استفاده از خدمات برخط خاص مثل سایت‌های شبکه اجتماعی اتفاق می‌افتد و درواقع در اینجا نگرش‌ها و رفتارها با یکدیگر در ارتباط هستند و آنچه که باعث افشای اطلاعات گذشته، تفاوت در دیدگاه کاربران است.

۳- فرضیه مطلوبیت اجتماعی^۱ حاکی از آن است که کاربران با توجه به گستره وسیع اینترنت به صورت آگاهانه، به بررسی مشکلات مربوط به مدیریت حریم شخصی اقدام می‌کنند. هنجارها، فشار گروهی و محدودیت‌های موقعیتی ممکن است ترسیم‌کننده نگرش‌های منعکس شده در پژوهش‌ها باشند. از این رو، گزارش رفتار آن‌ها، ممکن است منعکس‌کننده تصویر کاملاً متفاوتی باشد.

۴- فرضیه سواد حریم خصوصی برخط که در مورد سطح اطلاعات و دانش فردی کاربران اینترنت است. افراد ممکن است با وجود نگرانی در مورد حریم خصوصی‌شان، قادر به حفاظت از آن نباشند. نبود دانش و سواد حریم خصوصی کاربران اینترنت یکی از عواملی است که مانع از عکس‌العمل مناسب و درست افراد برای حفظ حریم خصوصی می‌شود و این امر تناقض در نگرش‌ها و رفتار آنان را توجیه می‌کند. به‌زعم دیدگاه تری و دیگران (۲۰۱۵: ۸) با توجه به نقشی که سواد حریم خصوصی برخط، می‌تواند در کنترل اطلاعات شخصی داشته باشد، برخورداری افراد از سواد حریم خصوصی برخط به آن‌ها برای حل کردن تناقض حریم خصوصی برخط کمک خواهد کرد.

سواد حریم خصوصی برخط

امروزه با ورود بشر به عصر اطلاعات، مفاهیم مختلف دچار تغییراتی شده‌اند، یکی از این مفاهیم، مفهوم سواد است که بسیار گسترش یافته و دیگر تنها به معنای خواندن و نوشتن نیست. سواد در عصر اطلاعات زیرشاخه‌های بسیاری مثل سواد اطلاعاتی، سواد رسانه، سواد رایانه، سواد دیجیتال و غیره دارد. سواد حریم خصوصی برخط یکی از ضروریات استفاده از اینترنت است که بسیار حائز اهمیت است. این سواد که خود یکی از ابعاد سواد دیجیتال است و در برخی منابع از آن تحت عنوان سواد اخلاقی-اجتماعی نیز یاد شده است به معنای فهم رفتار درست و معقول در محیط‌های دیجیتال و دربرگیرنده مسائل حریم خصوصی و امنیتی است (اشت-الکالای و آمیچی-هامبورگر^۲، ۲۰۰۴؛ بودن^۳، ۲۰۰۸؛ نقل از سیاسی‌راد و بیچرانلو، ۱۳۹۶: ۱۳۲). دباتین (۲۰۱۱: ۵۱) سواد حریم خصوصی را یک نگرانی آگاهانه برای حفظ حریم خصوصی و راهبردهای مؤثر برای محافظت از آن، تعریف می‌کند. در تعریفی دیگر، سواد حریم خصوصی برخط عبارت است از: سطح درک و آگاهی از نحوه ردیابی اطلاعات در محیط‌های برخط و چگونگی استفاده از اطلاعات (Givens, 2015; Quoted from Wissinger, 2017: 380).

1. Social desirability hypothesis

2. Eshel-Alkali & Amichai-Hamburger

3. Bawden

از تعاریف سواد حریم خصوصی برخط که صاحب نظران ارائه کرده اند می توان استنباط کرد که سواد حریم خصوصی برخط، یعنی یک نوع درک متکی بر مهارت که بر اساس آن می توان از حریم خصوصی برخط محافظت کرد.

ترپت و دیگران (۲۰۱۵: ۸) بیان داشتند که سواد حریم خصوصی برخط، دانش حفاظت از داده های شخصی و راهکارهای حفاظت از آن است و آن را ترکیبی از دانش واقعی^۱ یا روایتی^۲ (دانش چپستی^۳) و دانش فرایندی^۴ (دانش چگونگی^۵) درباره حفظ حریم خصوصی برخط، می دانند. با توجه به دانش واقعی، سواد حریم خصوصی برخط به دانش کاربران در خصوص جنبه های فنی حفاظت از اطلاعات برخط، قوانین و دستورالعمل ها حفاظت از اطلاعات برخط و همچنین آگاهی از شیوه ارائه دهندگان خدمات برخط اشاره دارد. از منظر دانش فرایندی، سواد حریم خصوصی برخط، شامل توانایی کاربران در خصوص اعمال راهکارهای برای کنترل حریم خصوصی و حفاظت از داده های شخصی است. برخورداری از دانش راهکارهای کنترل فردی حریم خصوصی از سوی کاربران در برخی مقیاس ها از الزامات برخورداری افراد از سواد حریم خصوصی برخط، قلمداد شده است. این راهکارها ترکیبی از مهارت های اجتماعی و فنی است (Trepte et al. 2015: 19; Park, 2013: 224). راهکارهای فنی حفظ حریم خصوصی، راهکارهایی است که کاربران از طریق آن ها از ابزارها یا امکانات یک سایت برای حفظ حریم خصوصی خود استفاده می کنند. درحالی که راهکارهای اجتماعی شامل ایجاد محدودیت های ذهنی در افشا می شود که با کمک آن کاربر فقط اطلاعاتی را افشا می کند که برای او خطری نداشته باشد (هogan^۶، ۲۰۱۰؛ نقل از سیاسی راد و بیچرانلو، ۱۳۹۶: ۱۳۳)؛ بنابراین سواد حریم خصوصی برخط می تواند بر رفتار کاربران اینترنت که نگران حریم خصوصی خود هستند، تأثیر گذاشته و با بهره گیری از دانش و راهکارهای لازم در جهت حمایت از داده های شخصی خود اقدام کنند.

ابعاد سواد حریم خصوصی برخط

ترپت و همکاران (۲۰۱۵: ۱۶-۱۹) با تحلیل محتوای کیفی متون مربوط به سواد حریم خصوصی برخط، مقیاسی را برای سنجش این سواد مطرح کردند که شامل پنج بعد مختلف بود که عبارتند از:

۱- آگاهی از شیوه سازمان ها، مؤسسات و ارائه دهندگان خدمات برخط: مردم در زندگی روزمره خود از انواع سیستم های عامل و وبسایت ها استفاده می کنند و برای این کار نیاز به افشای اطلاعات شخصی شان دارند. از این رو کاربران باید از چگونگی استفاده ارائه دهندگان خدمات برخط از اطلاعات شخصی افراد، درک کلی از جریان داده ها، نحوه انتقال و دریافت آن ها توسط مؤسسات و ذی نفعان

1. Factual

2. Declar

3. Knowing that

4. Procedural

5. Knowing how

6. Hogan

آگاهی داشته باشند. این آگاهی باعث می‌شود که در هنگام استفاده از آن‌ها به اعتبار و بیانیه‌ای حریم خصوصی وبسایت‌های مختلف توجه کنند.

۲- آگاهی از جنبه‌های فنی حریم خصوصی برخط و حفاظت از داده‌ها: بعد دوم به دنبال اندازه‌گیری دانش فنی افراد در زمینه حفاظت از داده‌های برخط است. این دانش به‌عنوان یک الزام مهم در رابطه با حفاظت از اطلاعات شناخته شده است. برای مثال کاربرانی که نمی‌دانند فایروال^۱ چیست، احتمالاً قادر به استفاده درست از آن نیستند. آگاهی از جنبه‌های فنی و ابزارهای جدید در مقابله با خطرات تازه‌ای که در مورد حریم خصوصی در اینترنت به وجود می‌آید افراد را در توانایی مقابله با آن‌ها یاری می‌رساند

۳- آگاهی از قوانین و جنبه‌های قانونی حفاظت از داده‌های برخط: شناخت مقررات قانونی یکی از الزامات مهم در استفاده از اینترنت و خدمات برخط است و افراد تنها در صورتی که حقوق شخصی خود را دانسته و از محدودیت‌های قانونی در مؤسسات تجاری و وبسایت‌ها باخبر باشند می‌توانند با تصمیمات آگاهانه نسبت به کنترل حریم خصوصی‌شان اقدام کنند؛ به عبارت دیگر وقوف افراد بر حقوق خویش به آن‌ها اجازه می‌دهد تا از این حقوق بهره‌مند شده و درصدد احقاق آن بپردازند.

۴- آگاهی از راهکارهای لازم برای کنترل حریم خصوصی: کاربران اینترنت علاوه بر آگاهی از شیوه ارائه‌دهندگان خدمات برخط، جنبه‌های فنی حفظ حریم خصوصی و آگاهی از قوانین مربوطه، باید بتوانند اقدامات و راهکارهای لازم را در جهت حفظ حریم خصوصی برخط به کارگیرند. برخلاف دیگر ابعاد سواد حریم خصوصی برخط، این بعد مربوط به دانش فرایندی می‌باشد به همین خاطر می‌توان آن را توانایی کنترل داده‌های شخصی دانست که شامل ترکیبی از مهارت‌های اجتماعی (به‌عنوان مثال، افشای اطلاعات شخصی را به حداقل برسانیم) و مهارت‌های فنی (استفاده از ابزارهای کنترلی، به‌عنوان مثال، پاک کردن حافظه پنهان مرورگر وب) است.

۵- آگاهی از دستورالعمل‌ها در مورد حریم خصوصی و حفاظت از داده‌ها: شناخت دستورالعمل‌های حفاظت از اطلاعات شخصی که برای راهنمایی شهروندان تهیه شده می‌تواند آن‌ها را در عملکرد بهتر در حفاظت از حریم خصوصی برخط یاری کند. این دستورالعمل‌ها لازمه‌ای برای استفاده و بهره‌گیری از امکانات اینترنت است تا افراد بتوانند با امنیت بیشتری در اینترنت عمل کنند.

تهدیدات حریم خصوصی برخط

آشنایی با خطرات و تهدیدهای حریم خصوصی برخط، باعث آگاهی افراد از روش‌هایی می‌شود که ممکن است حریم خصوصی‌شان مورد نقض قرار گیرد. موارد زیر از جمله مهم‌ترین خطراتی هستند که افراد لازم است با آن‌ها آشنایی داشته باشند.

۱- جعل اینترنتی (فیشینگ): فیشینگ در اصطلاح به معنای شبیه‌سازی قسمت‌هایی از یک سایت

1. Firewall

اینترنتی (مثلاً یک صفحه از سایت) آشنا یا معروف است که به وسیله آن بتوان کاربر را گمراه کرده و اطلاعات شخصی وی را به دست آورد. این اطلاعات می‌تواند شامل نام کاربری و کلمه عبور فرد در آن سایت یا اطلاعاتی مربوط به شمار حساب بانکی فرد و خیلی موارد دیگر (قیاسی، دوستار و توانبخش، ۱۳۹۶: ۱۱۹).

۲- ویروس^۱: ویروس‌ها برنامه‌هایی هستند که به انتهای برنامه دیگری متصل و یا وارد بدنه آن می‌شود. وقتی این برنامه به اجرا درمی‌آید، ویروس همراه آن اجرا شده، نسخه‌های خود را وارد فایل یا قسمت‌های دیگری از حافظه می‌کند و به این ترتیب نسخه‌های بیشتری منتشر می‌شوند. با هر بار اجرای یکی از فایل‌ها یا برنامه‌های آلوده، این روند تکرار می‌شود (علیزاده و انصاری، ۱۳۹۰: ۷۷).

۳- کرم^۲: کرم‌ها برخلاف ویروس‌ها برنامه‌های متکی به خود هستند و بدون نیاز به سایر برنامه‌ها فعالیت دارند؛ آن‌ها با کپی کردن از یک رایانه به رایانه دیگر روی شبکه تکثیر می‌شوند. یک کرم ویژگی‌های یک فایل را از بین می‌برد و این کار به او اجازه می‌دهد بی‌هدف به حرکت ادامه دهد. در نتیجه سرورهای شبکه، سرورهای وب و رایانه‌های شخصی از کار بازمی‌مانند (حسن‌زاده و جهانگیری، ۱۳۹۰: ۱۴۸).

۴- تروجان^۳ یا اسب تروا^۴: برنامه‌ای است که به ظاهر، قصد انجام یک کار بی‌خطر و موجه را دارد، ولی دارای کد مخفی است که عمل تخریب را انجام می‌دهد. تروجان، خودش را منتشر نمی‌کند، بلکه معمولاً برای کپی کردن خودش، از یک ویروس یا کرم استفاده می‌کند. یک مثال قدیمی، برنامه‌های لاگین^۵ برای سرقت رمز عبور هستند که یک درخواست به نظر موجه برای نام کاربری و رمز عبور نمایش می‌دهند و منتظر می‌مانند تا کاربر اطلاعات را وارد کند. سپس، برنامه سرقت‌کننده رمز عبور، «رمز عبور اشتباه» اطلاعات را درجایی برای سازنده آن مخفی می‌کنند و یک پیغام خطای نمایش می‌دهند و پس از آن برنامه واقعی لاگین اجرا می‌شود. (استالینگر، ۱۳۹۳: ۲۱۲).

۵- جاسوس افزار^۶: جاسوس افزارها نرم افزارهای جاسوس‌یابی هستند که بر روی رایانه نصب شده و اطلاعات موجود در رایانه مانند رمز عبور حساب‌های مختلف، شماره کارت‌های بانکی و غیره را به سازنده نرم افزار ارسال می‌کنند. کی لاگرها^۷ یکی از معروف‌ترین جاسوس افزارها هستند که اگر رایانه به آن آلوده شود تمامی جملاتی که در رایانه تایپ می‌شود را ضبط و به فردی که کی لاگر را تهیه کرده است ارسال می‌کند (مهارت‌هایی برای نویسنده قرن ۲۱، ۱۳۹۸: ۱۷۳).

۶- جعل هویت^۸: سرقت هویت زمانی واقع می‌شود که فردی از اطلاعات شخصی دیگری مانند

1. Virus
2. Worm
3. Trojan
4. Trojan horse
5. login
6. Spyware
7. Keyloggers
8. Identity Theft

نام، نام خانوادگی، شماره امنیت اجتماعی، شماره شناسنامه و غیره، به منظور جعل هویت دیگری، انجام خریدهای غیرقانونی، برداشت از حساب بانکی، افتتاح یک کارت اعتباری جدید با استفاده از اطلاعات دزدیده شده یا انجام سایر فعالیت‌های غیرقانونی، استفاده و بهره‌برداری می‌کند (Sanchez, 2012: 85).

۷- کوکی^۱: کوکی یک فایل کوچک متنی است که یک وب‌سایت در رایانه کاربر برای ذخیره اطلاعات مربوط به فعالیت او در سایت قرار می‌دهد و در هر بار بازدید از آن سایت، کوکی مربوط به آن سایت اجرا شده و محتوای آن به سایت مربوطه ارسال می‌گردد. این تکنیک در ابتدا برای راحتی کاربران طراحی شد. چراکه آن‌ها را از وارد کردن مکرر کد کاربری و رمز عبور در اتصالات متوالی به یک سایت بی‌نیاز می‌ساخت. ولی هم‌اکنون کوکی‌ها به عنوان طعمه‌ای جهت مهاجمان به شمار می‌روند (Lavin, 2006: 280).

راهکارهای حفظ حریم خصوصی برخط
 راهکارهای حفظ حریم خصوصی برخط باعث ارتقای توانایی افراد در حفاظت از حریم خصوصی شده و سواد حریم خصوصی برخط آنان را افزایش می‌دهد. موارد زیر از جمله مهم‌ترین مواردی هستند که کاربران اینترنت لازم است با آن‌ها آشنایی کافی داشته باشند.

۱- ضدویروس^۲: ضدویروس (آنتی‌ویروس) اصطلاحی است که به برنامه یا مجموعه‌ای از برنامه‌ها اطلاق می‌شود که برای محافظت از رایانه‌ها در برابر ویروس‌ها استفاده می‌شوند. وظیفه اصلی این برنامه‌ها شناسایی پرونده‌های آلوده به ویروس و پاک‌سازی آن‌هاست. در مواردی که این عمل ممکن نباشد، سازوکاری برای قرنطینه کردن پرونده آلوده وجود دارد و حتی می‌توان تنظیمات ضدویروس‌ها را به گونه‌ای انجام داد که پرونده آلوده حذف شود (عباسی و شکرریز، ۱۳۹۲: ۲۲۹).

۲- دیواره آتش^۳: دیواره آتش، ابزارها و نرم‌افزارهایی هستند که می‌توان قواعدی را از جهت صحیح یا غیر صحیح بودن ارتباطات (داخلی-خارجی و خارجی-داخلی) را کنترل کرد و در صورت وقوع یک امری خلاف اصول و قواعد تعریف شده باز به همان شکلی که برای آن تعریف گردیده از قبیل قطع ارتباط یا انحراف آن عمل نماید و حکم حصار را دارد که به دور بخشی که امنیت آن باید تأمین شود، کشیده می‌شود (اسکندری، ۱۳۹۰: ۸۲).

۳- پاک کردن تاریخچه مرور^۴: تاریخچه مرورگر اینترنت با هدف تسهیل برخی از امور ایجاد می‌شود، لیکن در بسیاری از مواقع ممکن است موجب نقض حریم خصوصی افراد گردد و با هدف جمع‌آوری بسیاری از اطلاعات شخصی و آسیب رساندن به افراد، مورد استفاده قرار گیرد. کاربران می‌توانند با حذف کردن تاریخچه مرورشان این تهدیدات را تا حدودی کاهش دهند.

1. cookie

2. Anti Virus

3. Firewall

4. Delete browser history

۴- ضد جاسوس افزار^۱: ابزاری است که علیه جاسوس افزارها به کار گرفته می شود. این ابزار به جای تمرکز بر ویروس ها، دیگر برنامه های خطرناک از جمله برنامه های جاسوسی و نظارتی را کشف و خنثی می کند.

۵- مرور خصوصی^۲: مرور خصوصی، یک حالت در مرورگر است که امکانی را برای حفظ اطلاعات شخصی کاربران در هنگام وب گردی ایجاد کرده است. در این حالت، مرورگر هرگز تاریخ مرور، کوکی ها، سابقه مرور کاربران را ذخیره نخواهد کرد؛ اما مرور خصوصی در مواردی ناتوان عمل می کند به عبارت دیگر مرور خصوصی تنها اطلاعات شخصی را حفظ می کند و آثار داخلی کاربران را پاک سازی می کند اما آدرس آی پی^۳ و دیگر اطلاعات قابل ردیابی باقی خواهند ماند (Ruiz, Amatte, Park & Winter, 2017: 1).

۶- تغییر رمز عبور^۴: مجرمان رمز عبورهای ضعیف را به کمک برنامه های ویژه شکستن رمز، حدس می زنند این برنامه ها با استفاده از الگوریتم های خاص و لغت نامه کلمات رایج، صدها یا هزاران رمز عبور را حدس می زنند. رمز عبورهای ضعیف مثل اسامی رایج، تاریخ تولد یا کلمات خاص به راحتی حدس زده می شوند. انتخاب رمز عبور هوشمندانه و ترکیبی از حروف و اعداد به جای رمز عبورهای پیش فرض و ساده می تواند مؤثر واقع شود (بنایی، سهامی و مختار، ۱۳۸۹: ۱۴).

راه رسیدن به سواد حریم خصوصی برخط

سواد حریم خصوصی برخط و آگاهی از اصول و ضوابط و اهمیت آن در دوره فعلی صرفاً از طریق آگاهی رسانی و آموزش اتفاق می افتد؛ به عبارت دیگر، سیستم های آموزشی باید به گونه ای طراحی شوند که هم واحدهایی برای آگاهی از خطرات برخط بودن مطرح شود و هم دانش آموزان و دانشجویان در کلاس های درس خود به صورت دائم و به مقدار کافی با راهکارهای حفاظت از حریم شخصی و قوانین مربوطه آشنا شوند.

اما مثل همیشه علم چند قدم جلوتر از انسان حرکت می کند و فرآیند تطبیق به همین سادگی ها اتفاق نمی افتد. نمونه بارز آن، وجود کلاس های درسی است که حتی از ساده ترین ابزارهای فناوری هم محروم هستند. کمبود آموزگاران و اساتیدی را که بتوانند دانش آموزان و دانشجویان را با سرعت دنیای دیجیتال و فناوری پیش ببرند هم به مسئله کمبود امکانات اضافه می شود. در این وضعیت بهتر است نگرانی هایمان نسبت به حریم خصوصی برخط بیشتر به این سمت سوق داده شود که اگر سواد حریم خصوصی برخط را به عنوان سواد ضروری در عصر دیجیتال در نظر بگیریم، نمی توانیم از حریم خصوصی مان حفاظت کنیم. همچنین در ایران تاکنون تحقیقات در عرصه سواد حریم خصوصی برخط انجام نشده و اهمیت آن برای سیاست گذاران حوزه آموزش کشور پوشیده مانده است. حتی در عرصه نهاد دانشگاه و به خصوص تحقیقات و پژوهش ها، تاکنون توجهی به سواد حریم خصوصی برخط و اهمیت آموزش آن به جوانان

1. Anti Spyware

2. private browsing

3. Internet Protocol (IP)

4. Change passwords

توجهی نشده است؛ درحالی که باید توجه داشته باشیم که یکی از اهداف دانشگاه، تربیت افرادی متخصص در عرصه رسانه است. تا با کسب شناخت کافی نسبت به سازوکار رسانه‌ها، سیاست‌های کلان حکومتی را در سطح جامعه بسط داده باشند و اینترنت به‌عنوان مهم‌ترین رسانه دارای خطرات و شرایطی است که نیاز به داشتن آگاهی در مورد استفاده از آن ضرورتی چشم‌پوشی‌ناپذیر است. ازاین‌رو توانایی حفظ حریم خصوصی در آموزش‌های حرفه‌ای امری ضروری است. نگرش آثاری در این حوزه مطالعاتی، به‌منظور آموزش شیو صحیح بهره‌گیری از سواد حریم خصوصی برخط و کاربرد مفید آن در فرآیندهای آموزشی می‌تواند تأثیر مطلوبی در حفظ حقوق شخصی باشد.

نتیجه‌گیری:

حریم خصوصی، یکی از حقوق اساسی بشر و مرتبط با حفظ مقام انسان و دیگر ارزش‌هایی است که کرامت انسانی بشر به ارمغان می‌آورد. امروزه با گسترش استفاده از اینترنت و به‌خصوص شبکه‌های اجتماعی که بر بستر اینترنت می‌باشد، حریم خصوصی به یکی از چالش‌برانگیزترین مسائل حقوق بشر تبدیل شده است به‌طوری‌که این ابزار از سوی افراد سودجو به گونه‌ای مورد استفاده قرار می‌گیرد که به بزرگ‌ترین نقض‌کننده حریم خصوصی افراد تبدیل شده است (خوش‌رفتار و محمدپور، ۱۳۹۶: ۳). با توجه به تهدیدهای فزاینده‌ای که از جانب افراد عادی جامعه، ارائه‌دهندگان خدمات اینترنتی و دولت‌ها علیه حریم خصوصی برخط افراد وجود دارد و همچنین گسترش روزافزون استفاده از شبکه‌های اجتماعی، تجارت الکترونیک در سال‌های اخیر، ضرورت حمایت از حریم خصوصی در عصر حاضر بیش از پیش احساس می‌شود. نبود سواد لازم برای استفاده صحیح از این فضای پیش‌رو و از طرف دیگر ضعف آموزش‌های لازم به افراد جامعه در راستای حمایت از حریم خصوصی افراد و عواملی از این قبیل موجب گردیده است که برخط بودن به خطری برای نقض حریم خصوصی افراد منجر شود. در این مقاله، ما استدلال کردیم که سواد حریم خصوصی برخط می‌تواند باعث جلوگیری از تناقض حریم خصوصی برخط شود. افرادی که در مورد حریم خصوصی خود نگران هستند و تمایل به حفاظت از اطلاعات شخصی‌شان دارند می‌توانند با بهره‌گیری از دانش در مورد راهکارهای کنترل حریم خصوصی، قوانین مربوطه که اطلاع از آن‌ها هنگام استفاده از اینترنت و نیز موقع نقض حریم خصوصی برخط، عامل مهمی در دفاع از حقوق است، جنبه‌های فنی و همچنین شیوه‌های نهادهای ارائه‌دهنده خدمات برخط در مورد نحوه استفاده از اطلاعات شخصی افراد، به‌طور مؤثر از حریم خصوصی خود محافظت کنند. بر این اساس، کاربران اینترنت ابتدا بایستی درباره مخاطرات و پیامدهای افشای اطلاعات محرمانه و نقض حریم خصوصی خودآگاهی و شناخت کافی داشته باشند، سپس راهکارهای حفظ اطلاعات محرمانه را به کارگیرند و به‌طور مستمر فرآیند آگاهی و شناخت سواد حریم خصوصی برخط را جهت حفظ حریم

خصوصی به عنوان یک سواد ضروری در عصر دیجیتال مورد توجه قرار دهند. به بیانی دیگر، فقدان آگاهی، نبود مهارت و ناتوانی در حفظ حریم خصوصی برخط می تواند پیامدهای اخلاقی و بحران های اجتماعی گاه جبرانناپذیری را برای کاربران و عموم افراد جامعه به دنبال داشته باشد. با در نظر گرفتن این شرایط، لازم است تا ما به طور دقیق نسبت به حریم خصوصی خود حساس بوده و اقدامات لازم را به منظور افزایش سطح سواد حریم خصوصی برخط به کاربندیم و با استفاده از آن با روش های امنیتی در فضای اینترنت محیط آن را امن تر کنیم. غالباً دولت ها قادر به حمایت مستقیم از شهروندان خود در زمینه جرائم ارتكابی در فضای مجازی نمی باشند، اما می توانند با وضع قوانین حمایت از حریم خصوصی برخط افراد و ایجاد شرایط و بستری لازم در جهت ارتقاء سواد حریم خصوصی برخط شهروندان، آموزش افراد را در جامعه تسهیل نمایند.

از این رو برای رسیدن به سواد حریم خصوصی برخط، آموزش آن امری ضروری است. نهادهای آموزشی مثل مدارس، دانشگاه ها و آموزشگاه های مختلف می توانند مفهوم سواد حریم خصوصی برخط را در کتب درسی ارائه کنند و از طریق افزایش تدابیر آموزشی و بسط مهارت های امنیتی می توان خطرات نقض حریم خصوصی در فضای مجازی را کاهش دهند. لذا، دستیابی به سواد حریم خصوصی برخط مستلزم برنامه ریزی دقیق و تدوین رویکردها و راهبردهای تازه و نوآورانه بسیاری است تا بتوان در سال های آینده به این مقصد رهنمون شد.

پیشنهادهای:

در این بخش برخی پیشنهادهایی برای ارتقای سواد حریم خصوصی برخط شهروندان به اختصار بیان می شود:

۱- تدوین و انتشار جزوات و کتاب های ویژه آموزش سواد حریم خصوصی برخط برای همه اقشار مختلف جامعه.

۲- نهادهای فرهنگی و آموزشی مثل کتابخانه ها، با آموزش سواد حریم خصوصی برخط درگیر و مشارکت صمیمانه و مسئولانه ای را آغاز کنند.

۳- جذب افراد آموزش دیده و متخصص در امور رایانه ای در مدارس و دانشگاه ها جهت آموزش سواد حریم خصوصی برخط.

۴- فعال نمودن انجمن های اولیا و مربیان در زمینه آگاهی بخشی درباره آسیب های نوپدید فضای مجازی و تهدید حریم خصوصی در این حوزه.

۵- لازمه آموزش سواد حریم خصوصی برخط این است که عملکرد کشورهای پیشگام در این زمینه بررسی شود و سپس با ایده گرفتن از این اقدامات، آن ها را برای استفاده در کشورمان به کارگیریم.

۶- رسانه ها نیز می توانند در راستای ایفای نقش های خبری و آموزشی خود و شناخت صحیح

نیازهای مخاطبان، با استفاده از کارشناسان، مخاطبان را آموزش داده و در زمینه حفظ حریم خصوصی فرهنگ سازی کنند.

۷- دولت و مسئولین نیز می توانند با تدوین سیاست ها و قوانین و همچنین ایجاد شرایط و بسترهای لازم در راستای افزایش سواد حریم خصوصی برخط افراد جامعه اقدام نمایند.

۸- توجه به تناسب آموزش های سواد حریم خصوصی برخط با گروه های سنی مختلف ضروری به نظر می رسد.

۹- برگزاری کارگاه های آموزشی مهارت های سواد حریم خصوصی برخط در مدارس و دانشگاه ها می تواند در افزایش سطح سواد حریم خصوصی برخط نوجوانان و جوانان مؤثر واقع شود.

۱۰- پژوهش هایی در مورد راهکارهای مفید برای رشد و توسعه مهارت های سواد حریم خصوصی برخط کاربران مختلف اینترنت انجام گیرد.

منابع

- استالینگز، ویلیام (۱۳۹۳). **اصول و مبانی امنیت شبکه: کاربردها و استانداردها**. ترجمه آرش حبیبی لشکری و نسرين بدیع. تهران: علوم ایران.
- اسکندری، حمید (۱۳۹۰). **دانشتنی‌های پدافند غیرعامل ویژه دوره عمومی سطح ۲**. تهران: بوستان حمید.
- بنایی، سجاد؛ سهامی، سهیلا و مختار، سمیرا (۱۳۹۸). **انواع حملات در فضای سایبر**. تهران: سازمان فناوری اطلاعات ایران.
- حبیبی، همایون (۱۳۹۵). «**حق بر حریم خصوصی در شبکه‌های اجتماعی**». تحقیقات حقوقی، ۱۹(۷۵)، ۳۹-۶۴.
- حسن‌زاده، محمد و جهانگیری، نرگس (۱۳۹۰). **امنیت اطلاعات: از آگاهی تا آموزش**. تهران: کتابدار.
- خوش‌رفتار، محمدحادی و محمدپور، سارا (۱۳۹۶). «**نقش استفاده از شبکه‌های اجتماعی تلگرام و واتساپ بر حریم خصوصی از دید کاربران**». پژوهش اجتماعی، ۹(۳۶)، ۱۹-۲۳.
- سیاسی‌راد، فرزانه و بیچرانلو، عبدالله (۱۳۹۶). «**الگوهای به‌کارگیری راهبردهای سواد حرم خصوصی آنلاین؛ مطالعه موردی کاربران دختر اینستاگرام**». فصلنامه تحقیقات فرهنگی ایران، ۱۰(۳)، ۱۲۵-۱۵۱.
- عباسی، محمدعلی و شکرریز، محمدرضا (۱۳۹۲). **مبانی و کاربرد رایانه**. تهران: مدرسه.
- عتقی، عبدالغنی (۱۳۹۷). **بررسی تطبیقی سیاست کیفری ایران و سوریه در حمایت از داده‌های شخصی با نگاهی به حقوق انگلستان**. پایان‌نامه کارشناسی ارشد. گروه حقوق. دانشکده حقوق و علوم سیاسی. دانشگاه فردوسی مشهد.
- عزیززاده، نوید و انصاری، زهرا (۱۳۹۰). «**بداافزارها و چالش‌های ایمنی در محیط سایبر**». نشریه نشاء علم، ۲(۱)، ۷۶-۸۰.
- فتحی، یونس و شاهمادی، خیرالله (۱۳۹۶). «**گستره و قلمرو حریم خصوصی در فضای مجازی**». حقوقی دادگستری، ۸۱(۹۹)، ۲۲۹-۲۵۲.
- قیاسی، رضا؛ دوستار، محمد و توانبخش، جعفر (۱۳۹۶). «**تحلیل راهکارهای مواجهه با فعالیت‌های فیشینگ در بانکداری الکترونیکی**». فصلنامه پژوهش‌های اطلاعاتی و جنایی، ۱۲(۱)، ۱۱۵-۱۳۱.
- محسنی، فرید و صوفی زمر، محسن (۱۳۹۶). «**پلیس و چالش‌های اجرایی تأمین امنیت سایبری**». علوم اجتماعی: دانش انتظامی، ۷۷(۷۷)، ۱۶۳-۱۸۸.
- محسنی، فرید و قاسم‌زاده، فریدون (۱۳۸۵). «**حریم شخصی در فضای مجازی، با تکیه بر حقوق ایران**». فصلنامه شریف، ۳۴(۳)، ۳۰-۲۱.
- مهارت‌هایی برای نویسنده قرن ۲۱ (۱۳۹۸). گروه نویسندگان. تهران: نشر نوگام.
- Bartsch, M. & Dienlin, T. (2016). **“Control your Facebook: An analysis of online privacy literacy”**. Computers in Human Behavior, 56, 147-154.

- Debatin, B. (2011). **Ethics, privacy, and self-restraint in social networking**. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47–60). Berlin, Germany: Springer.
- Lavin, M. (2006). “**Cookies: What Do Consumers Know and What Can They Learn?**”. *Journal of Targeting, Measurement and Analysis for Marketing*, 14 (4), 279–88.
- Maceli, M. G. (2018). “**Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries**”. *International Federation of Library Associations and Institutions*, 44(3), 195–202.
- Park, Y.J. (2013). “**Digital literacy and privacy behavior online**”. *Communication Research*, 40 (2), 215-236.
- Rotman, D. (2009). “**Are you looking at me? Social media and privacy literacy**”. Poster presented at the iConference, Chapel Hill, NC. February 8–11.
- Ruiz, R. D. S. Amatte, F. P. Park, K. J. B. & Winter, R. (2015). “**Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode**”. *IJCSDF*, 4(3), 404-416.
- Sanchez, M. (2012). “**The role of the forensic accountant in a medicare fraud identity theft case**”. *Global Journal of Business Research*, 6(3), 85-92.
- Trepte, S. Teutsch, D. Masur, P.K. Eicher, C. Fischer, M. Hennhöfer, A. & Lind, F. (2015). “**Do people know about privacy and data protection strategies? Towards the ‘online privacy literacy scale’(OPLIS)**”. in Gutwirth, S. Leenes, R. and de Hert, P. (Eds), *Reforming European Data Protection Law*, Springer, Dordrecht. 333-365.
- Veghes, C. Orzan, M. Acatrinei, C. & Dugulan, D.) 2012). “**Privacy literacy: what is and how it can be measured?**”. *Annales Universitatis Apulensis Series Oeconomica*, 14(2), 704 – 712.
- Weinberger, M. Bouhnik, D. & Zhitomirsky-Geffet, M. (2017). “**Factors affecting students’ privacy paradox and privacy protection behavior**”. *Open Information Science*, 1(1), 1-18.
- Weinberger, M. Zhitomirsky-Geffet, M. & Bouhnik, D. (2017). “**Factors affecting users’ online privacy literacy among students in Israel**”. *Online Information Review*, 41(5), 655-671.
- Wissinger, C.L. (2017). “**Privacy literacy: From theory to practice**”. *Communications in Information Literacy*, 11(2), 378-389.
- Youn, S. (2009). “**Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents**”. *The Journal of Consumer Affairs*, 43(3), 389-418.