سال سیزدهم، شماره‌های۴۹و۵۰، پاییز و زمستان ۱۴۰۰

صص: ۱۷۳_۱۸۲

دو فصلنامه علمی

فناوری اطلاعات و ارتباطات ایران

بررسی نقش شخصیت و متغیرهای فردی بر نقض امنیت رمز عبور: یک مطالعه تجربی

زهرا کریمی[1]* منیژه کاوه رضوان صالحی** میلاد ملتجی*****

* استادیار گروه علوم کامپیوتر، دانشگاه شهرکرد

** استادیار گروه مشاوره و روانشناسی، دانشگاه شهرکرد

*** دانش‌آموخته کارشناسی علوم کامپیوتر، دانشگاه شهرکرد

تاریخ دریافت: ۱۳۹۹/۱۲/۱۲ تاریخ پذیرش: ۱۴۰۰/۰۵/۱۹

نوع مقاله: پژوهشی

چکیده

تفاوت‌های فردی کاربران فناوری اطلاعات در انتخاب رمز عبور و نگهداری از آن تأثیرگذار است. در این راستا، این مطالعه، رابطه بین متغیرهای جنسیت، شخصیت، میزان تحصیلات و رشته تحصیلی از یک طرف و نقض امنیت رمز عبور را از طرف دیگر در بین کاربران ایرانی بررسی کرده است. روش پژوهش حاضر، روش توصیفی از نوع همبستگی بود. نمونه‌ای با استفاده از روش نمونه‌گیری در دسترس انتخاب شد که به پرسش‌نامه‌های پنج عامل بزرگ شخصیتی نئو، اطلاعات جمعیت شناختی و رفتارهای امنیت رمز عبور پاسخ دادند. داده‌ها با استفاده از ضریب همبستگی پیرسون، آزمون تی‌دو، آنوا و تحلیل رگرسیون (برای ۵۲۹ مورد پرسش‌نامه قابل قبول) مورد تحلیل قرار گرفتند. نتایج نشان داد که کاربران مرد نسبت به کاربران زن؛ رمز عبورهای قوی‌تری انتخاب می‌کنند. رفتارهای نقض‌کننده امنیت رمز عبور در کاربران رشته‌های تحصیلی علوم ریاضی، حسابداری و کامپیوتر نسبت به کاربران در سایر رشته‌های تحصیلی بیش‌تر تکرار شده است. از بین ویژگی‌های شخصیت، روان‌نژندگرایی رابطه مثبت و معنادار، تجربه‌پذیری و توافق‌پذیری رابطه منفی و معنادار و وجدان‌گرایی رابطه دوگانه با ویژگی نقض امنیت رمز عبور دارد. این یافته‌ها با در نظر گرفتن تفاوت فردی در زمینه رفتارها و ادراکات امنیتی، به حوزه امنیت سایبری به‌ویژه در ایران کمک می‌کند.

واژگان کلیدی: امنیت سایبری، رمز عبور، شخصیت، جنسیت، رشته تحصیلی، تحلیل همبستگی.

۱. مقدمه

جرایم سایبری[2]، مشکلی همیشگی بوده و افزایش قربانیان آن در سال‌های اخیر، هشداردهنده بوده است. گزارش‌های موجود حاکی از این است که شکست‌های امنیتی نسبت به سال ۲۰۱۴ افزایش ۶۷٪ داشته و نسبت به سال ۲۰۱۸ نیز ۱۱٪ رشد کرده‌اند. پیش‌بینی شده که خسارت‌های جرایم سایبری در سال ۲۰۲۲ به بیست برابر میزان این جرائم در سال ۲۰۲۰ یعنی حدود ۱۳۳/۷ دلار افزایش یابد[3].

[1] نویسنده مسئول: زهرا کریمی zahra.karimi@sku.ac.ir

[2] Cybercrime

[3] https://www.cyber-observer.com/cyber-news-۲۹-statistics-for-۲۰۲۰-cyber-observer/, دسترسی شده در مهرماه ۱۳۹۹

عوامل نرم شـــامل عوامل مدیریتی، فرهنگی و اجتماعی نســـبت به عوامل سخت شامل عوامل مالی و فنی/فناورانه در امنیت سایبری از اهمیت بیش‌تری برخوردار هستند [۱]. و در بین عوامل نرم، انسان، به عنوان عامل مهمی‌در نقض امنیت سایبری به ر سمیت شناخته شده است [۲]. در واقع انسان، ضعیف‌ترین حلقه موجود در زنجیره امنیت سایبری مح سوب می شود و در صورت انجام اقدام در ست می‌تواند به قوی‌ترین سرمایه امنیتی تبدیل شود [۳].

رفتارهای امنیتی کاربران ممکن اســت به خط مشـــی‌ها، ارزش‌ها و اســـتانداردهای موجود در ســـازمان، رفتارهای مدیریت ارشـــد و همکاران [۴]، میزان آگاهی [۵] یا آموزش افراد مربوط با شد. واضح اســـت که با وجود همه‌ی تمهیدات باز هم افراد با هم فرق دارند. بع ضی از افراد ممکن ا ست با وجود همه‌ی آموزش‌ها و سیا ست‌ها همچنان رفتارهای ضعیف‌تری نسبت به سایر افراد داشته باشند. از آن‌جا که درک تفاوت های فردی کاربران که بر تصـــمیم‌گیری و اجرای یک رف تار امنیتی خاص اثر گذار اســـت، بررســـی نقش تفاوت‌های فردی در امنیت سایبری، امکان سفار شی سازی آموزش امنیتی برای بهبود عواقب را فراهم می‌کند[۶].

برخی پژوهش‌ها به بررسی این تفاوت‌ها پرداخته‌اند. از جمله این‌که نقش جن سیت را در این حیطه، مورد مطالعه قرار داده‌اند. یافته‌های پژوهش‌های قبلی نشـــان داده‌اند که زنان، خیلی بیش‌تر از مردان از رمزهای یک سان در کاربردهای مختلف ا ستفاده می‌کنند. همچنین، افراد در گروه ســـنی ۱۸-۲۴ ســـال، با احتمال بیش‌تری از دیگر گروه‌های سنی، از رمزهای یک سان در کاربردهای مختلف ا ستفاده می‌کنند و اغلب آن ها پذیرفته‌اند که از رمز های خود در چندین سایت استفاده کرده‌اند[۷].

پژوهش‌های دیگر، متغیر فردی دیگری مثل سن را بررسی کرده‌اند. مطالعات جمعیت شناختی و آ سیب‌پذیری در برابر دزدی سایبری[۱] (هنگامی‌که شخصی تلاش می‌کند دیگری را فریب دهد تا اطلاعات شخصی او را در اختیارش بگیرد؛ دزدی سایبری رخ داده‌است) نشان می‌دهند که آ سیب‌پذیری به دزدی سایبری، بین گروه‌های سنی و جنســـیت‌های مختلف، متغیر اســـت: افراد گروه ســـنی ۱۸-۲۵، بیش‌ترین آسـیب‌پذیری را به حملات دزدی سـایبری دارند [۸]. در یک برر سی از دزدی سایبری[۹] نشان داده شد که افراد جوان‌تر، مخصـــوصـــاً دانشـــجویان، به‌خاطر داشـــتن تجارب منفی کمتر از فریب‌کاری‌های آنلاین، آســـیب‌پذیری بیش‌تری به دزدی ســـایبری دارند. حمله‌ی دزدی سایبری در پژوهشی با مقیاس بزرگ (۱۰۹۱۷ عضو از دانشگاه)، برر سی شد و نتایج متناقض با یافته‌های قبلی در مورد ســـن به‌دســـت آورد و پیشـــنهاد می‌کند که عوامل جمعیت شناختی سن و جنسیت، به تنهایی قادر به پیش‌بینی آ سیب‌پذیری کاربر در دزدی‌های ســـایبری نیســـتند [۱۰]. در زمینه پیشـــینه آموز شی، پژوهش‌های قبلی دریافته‌اند که دانشجویان هنرهای آزاد، آسیب‌پذیری بیش‌تری به حملات دزدی سایبری دارند تا دانشجویان علوم و فناوری [۱۱].

پژوهش‌های چندی نشان می‌دهد که از بین متغیرهای فردی، ویژگی‌های شخصیتی ممکن است بر نحوه تعامل افراد با فناوری تأثیر بگذارند. شخصیت شامل پنج عامل N، E، O، A و C است: نمرات بالا در N (روان‌نژندگرایی[۲]) نشان می‌دهند چقدر افراد، احساسات منفی مثل عصبانیت، اضطراب و ناامیدی را تجربه می‌کنند. نمرات بالا در E (برون‌گرایی[۳]) نشان می‌دهند چقدر افراد به دنیای بیرون علاقمند هستند، با دیگران ارتباط برقرار می‌کنند و جسارت دارند. نمرات بالا در O (تجربه‌پذیری[۴]) نشان می‌دهند که چقدر افراد خلاق و هنردوست هستند، چقدر به تجربه‌ی چیزهای جدید علاقمند هستند و چقدر به احساسات خود و دیگران توجه می‌کنند. نمرات بالا در A (توافق‌پذیری[۵]) نشان می‌دهند چقدر افراد فروتن هستند و به هماهنگ شدن با دیگران اهمیت می‌دهند. چقدر ملاحظه‌کار، مهربان، دوستانه و بخشنده هستند. نمرات بالا در C (وجدان‌گرایی[۶]) نشان می‌دهند چقدر افراد رفتار برنامه‌ریزی‌شده، انضباط شخصی، وظیفه‌شناسی و هدف‌مندی را ترجیح می‌دهند.

یافته‌های پژوهش [۱۲] نشان داد که دو عامل شخصیت وظیفه شناسی و توافق‌پذیری با رفتارهای امنیت مربوط به فناوری اطلاعات دارند. در حالی که نتایج پژوهش دیگر [۱۳] نشان می‌دهد که ممکن است عوامل دیگری به جز شخصیت نیز بر قدرت رمزهای عبور آنلاین انتخاب شده یا ایجاد شده تاثیر داشته باشند. با این حال یافته‌هایی به‌دست آوردند که نمرات بالاتر در عامل‌های شخصیتی تجربه‌پذیری و برون‌گرایی رمزهای عبور کوتاه‌تری را پیش بینی می‌کردند که حاوی حروف کمتری بود و اعداد و نمادهای بیش‌تری داشتند، در حالی که نمرات بالا در عامل شخصیتی وظیفه‌شناسی وجود نمادهای کمتر در رمزهای عبور پیش بینی می‌کردند. برون‌گرایی به طور منفی با قدرت رمز عبور ارتباط داشت. عامل شخصیت تجربه‌پذیری به‌طور مثبت با توانایی تشخیص بین رمز عبور قوی و ضعیف ارتباط دارد.

یکی از مطالعات به این نتیجه رســـیده که قربانیان زن در دزدی ســـایبری، نمره بالایی در روان‌نژندی داشـــته و هیچ همبســـتگی معناداری بین مردان و این خصـوصـیت دیده نشـد [۱۴]. همچنین مشـخص شـد که افراد با نمره بالای تجربه‌پذیری، معمولاً اطلاعات بیش‌تری در فیســـبوک[۷] به اشـــتراک گذاشـــته و تنظیمات حریم خصـــوصـــی باز بیش‌تری دارند که می‌تواند آن ها را به حملات

[۱] Phishing
[۲] Neouroticism
[۳] Extraversion
[۴] Openness to Experience
[۵] Agreeableness
[۶] Conscientiousness
[۷] Facebook

آسیب‌پذیرتر کند. برعکس، در مطالعه دیگری مشخص شد که برون‌گرایی و تجربه پذیری بالا، با کاهش آسیب پذیری در برابر دزدی سایبری رابطه دارند [۱۵]. این تناقض، گیج‌کننده است، زیرا به نظر می‌رسد افراد برون‌گرا و تجربه‌پذیر، با احتمال بیش‌تری به ایمیل‌های احراز هویت‌نشده اعتماد می‌کنند.

شایان ذکر است که رفتارهای امنیت سایبری فراتر از رمز عبور هستند [۱۶]. بی‌توجهی به امن سازی دستگاه‌ها یعنی قفل نکردن رایانه شخصی و صفحه نمایش تلفن و عدم توجه به نصب وصله[۱]های امنیتی و به‌روزرسانی‌ها نیز جزء رفتارهای نقض‌کننده امنیت سایبری در بین کاربران هستند. همچنین عدم آگاهی فعال[۲] از تهدیدات امنیت سایبری یعنی بی‌توجهی کاربران به نشانه‌های زمینه‌ای مانند آدرس URL یا دیگر علائم مرورگر در صفحات وب یا پیام‌های ایمیل و توجه زیاد در زمان ار سال اطلاعات در صفحات وب و فعال بودن در گزارش‌دهی حوادث امنیتی و عدم به‌روزنگهداشتن نرم افزارها نیز زیرمجموعه‌ای از رفتارهای ناایمن است [۱۷].

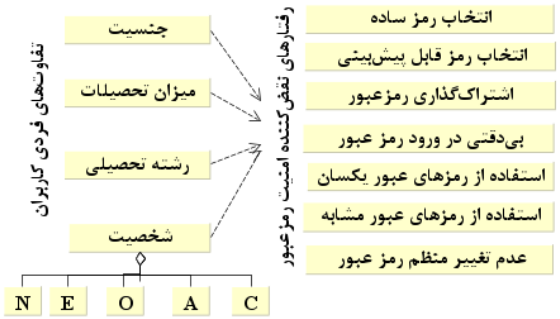
به طور خلاصه بررسی تفاوت‌های فردی موثر در رفتارهای امنیت سایبری که موضوع پژوهش جاری است، یک مسأله جالب پژوهشی است. در این پژوهش جهت تمرکز بهتر و بررسی دقیقتر از بین رفتارهای امنیت سایبری، رفتارهایی که به رمز عبور مربوط هستند، مدنظر قرار گرفته است.

بنا بر دانش ما تا کنون پژوهشی در این خصوص، در ایران انجام نشده است. به‌ویژه پژوهشی که تمام متغیرهای ذکر شده را مورد بررسی قرار داده باشد در این خصوص یافت نشد. لذا، نتایج پژوهش حاضر تا حدی خلأ پژوهشی این حیطه را پر خواهد کرد و یافته‌های حاصل از این پژوهش برای کابران فناوری اطلاعات و ارتباطات به ویژه کاربران ایرانی مفید خواهد بود. بنابراین مطالعه عوامل مؤثر بر چنین رفتارهای امنیتی ارزشمند و ضروری است.

در ادامه، ابتدا در بخش دو، سؤال‌های پژوهش بیان شده، در قسمت سه روش پژوهش توصیف شده و در بخش چهار نتایج پژوهش گزارش می‌شوند. در نهایت در بخش پنج نتایج مورد بحث قرار گرفته و در بخش شش نتیجه‌گیری ارائه می‌شود.

۲. بیان مساله

همان‌طور که اشاره شد در این پژوهش بر روی تفاوت کاربران ایرانی در حوزه رفتارهای نقض‌کننده امنیت رمز عبور مطالعه می‌شود. این تفاوت با در نظر گرفتن عامل‌های جنسیت، شخصیت، میزان تحصیلات و رشته تحصیلی سنجیده می‌شود. این متغیرها و ارتباط آن‌ها با انواع رفتارهایی که امینت رمز عبور را نقض می‌کنند در شکل ۱ نشان داده شده است.



شکل ۱. مدل ارتباطی متغیرهای پژوهش

همان‌طور که در شکل ۱ مشخص است رفتارهای نقض‌کننده امنیت رمز عبور شامل موارد زیر هستند:

رفتار یک-انتخاب رمز ساده: افراد با انتخاب رمزهای ساده مثل انتخاب نکردن علائم و حروف می‌توانند امنیت رمز عبور را نقض کنند.

رفتار دو-انتخاب رمز قابل پیش‌بینی: کاربران با انتخاب اسم یا شماره شناسایی خودشان و دوستان‌شان، این بستر را فراهم می‌کنند که دیگران به سادگی رمز آن‌ها را پیش‌بینی کنند.

رفتار سه-اشتراک‌گذاری رمزعبور: با در میان گذاشتن رمزعبور با دوستان و خویشان، محرمانگی و امنیت رمز عبور نقض می‌شود.

رفتار چهار-بی‌دقتی در ورود رمز عبور: ممکن است در هنگام ورود رمز عبور، افراد دیگر متوجه رمز شوند. یا این‌که کاربران رمز را فراموش کرده باشند و چندین بار رمزهای نزدیک به هم وارد کنند و به این ترتیب به هکرها فرصت سوء استفاده دهند.

رفتار پنج- استفاده از رمزهای عبور یکسان: کاربران با استفاده از یک رمز یکسان در جاهای مختلف، می‌توانند امنیت رمز عبور خود را نقض کنند.

رفتار شش-استفاده از رمزهای عبور مشابه: کاربران با استفاده از رمزهای مشابه در جاهای مختلف ممکن است باعث نقض امنیت رمز عبور شوند.

رفتار هفت-عدم تغییر منظم رمز عبور: کاربران با تغییرندادن رمز عبور خود در طول زمان می‌توانند امنیت رمز عبور خود را نقض کنند.

با در نظر گرفتن روابط موجود در شکل ۱ سوال‌های زیر مدنظر قرار می‌گیرند:

سوال اول پژوهش- آیا جنسیت کاربر ایرانی بر میزان استفاده از رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟

سوال دوم پژوهش- آیا میزان تحصیلات کاربر ایرانی بر میزان تکرار رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟

[۱] patch

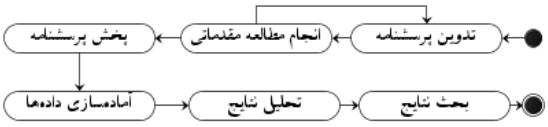
[۲] Proactive awareness

سوال سوم پژوهش-آیا رشته تحصیلی کاربر ایرانی بر میزان تکرار رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟

سوال چهارم پژوهش-آیا پنج عامل اصلی شخصیت کاربر ایرانی بر میزان تکرار رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟

۳. روش پـــژوهش

روش پـــژوهش از نـــوع توصـــیفی (غیرآزمایشـــی) - همبستگی است که روندنمای آن در شکل ۲ نشان داده شده است.



شکل ۲. روندنمای پژوهش

همان‌طور که در شـــکل یک مشـــاهده می‌شـــود در اولین مرحله ابزارهای لازم پژوهش یعنی پرســـش‌نامه تنظیم شـــد. پرســـش‌نامه دارای سه بخش زیر است:

جدول ۱. اطلاعات توصیفی افراد نمونه

متغیر	توصیف مقادیر داده‌ها
سن	۳ نفر زیر ۱۸ سال، ۱۹۹ نفر بین ۱۸ تا ۲۰ سال و ۲۰۸ نفر بین ۲۱ تا ۲۳ سال، ۶۲ نفر بین ۲۴ تا ۲۶ سال، ۲۴ نفر بین ۲۷ تا ۲۹، ۱۷ نفر بین ۳۰ تا ۳۴ و ۷ نفر بالای ۳۵
جنسیت	۱۴۹ مرد و ۳۸۰ زن
رشته تحصیلی	۱۳۵ نفر رشته‌های ادبیات و علوم انسانی، ۶۱ نفر رشته‌های فنی و مهندسی، ۲۰ نفر رشته‌های منابع طبیعی و علوم زمین، ۴۳ نفر رشته‌های علوم ریاضی، ۶۵ نفر رشته نقشه‌کشی معماری و طراحی دوخت، ۱۷ نفر رشته دامپزشکی، ۵۹ نفر رشته‌های کشاورزی، ۳۰ نفر رشته‌های علوم پایه، ۳۵ نفر رشته حسابداری و بازرگانی، ۶۱ نفر رشته کامپیوتر و فن‌آوری اطلاعات
میزان تحصیلات	۴۲۲ نفر کارشناسی، ۴۶ نفر کارشناسی ارشد، ۶۱ نفر دکترای حرفه‌ای یا تخصصی

بخش اول-پرســش‌نامه جمعیت‌شــناختی که در آن علاوه‌بر اطلاعات جنسیت، سن، میزان تحصیلات و رشته تحصیلی نیز از افراد پرسیده شد.

بخش دوم-پر ســـــــش‌نامه پنج عامل بزرگ شخصیتی نئو، برای ســـنجش ویژگی‌های شخصیتی: در یک دور از اجرای این پژوهش در جمع‌آوری دستی، از فرم کوتاه پرســـش‌نامه‌ی پنج عاملی شـــخصیت نئو (FFI-NEO) که شـــامل ۶۰ سؤال اســـت استفاده شد. این پرســـش‌نامه بر اساس تحلیل عاملی نمرات NEO-PI که در سال ۱۹۸۶ اجرا شده بود، به‌دست آمده است و پنج بعد عمدهٔ شخصیت را اندازه می‌گیرد که عبارت‌اند از روان‌نژندگرایی (N)، برون‌گرایی (E)، تجربه‌پذیری (O)، توافق‌پذیری (A) و وجدان‌گرایی (C). در هنجاریابی آزمون نئو که توسط گروسی فرشی [۱۸] انجام شد، ضرایب آلفای کرونباخ در هر یک از عوامل اصلی روان‌نژندگرایی، برون‌گرایی، توافق‌پذیری، تجربه‌پذیری و وجدان‌گرایی به‌ترتیب اعداد ۰/۸۶، ۰/۷۳، ۰/۵۶، ۰/۶۸ و ۰/۸۷ به‌دست آمد. در دورهای بعدی اجرای این پژوهش از فرم کوتاه‌تری با ۲۱ سؤال استفاده شد که توسط خرمائی و فرمانی [۱۹] هنجاریابی شده است. در هنجاریابی آن‌ها ضرایب آلفای کرونباخ در هر یک از عوامل اصلی روان‌نژندگرایی، برون‌گرایی، توافق‌پذیری، تجربه‌پذیری و وجدان‌گرایی به ترتیب اعداد ۰/۸۳، ۰/۸۳، ۰/۸۱، ۰/۷۲ و ۰/۶۹ به‌دست آمد.

بخش سوم-پرسش‌نامه محقق ساخته برای سنجش امنیت رمز عبور: پرسش‌نامه این پژوهش توسط نویسندگان تدوین شد به این صورت که در چند مرحله در جلسه‌های مشترک، پرسش‌های مناسب از مطالعات قبلی [۷]، [۱۷] و [۲۰] انتخاب، ترجمه، بومی‌سازی و بازنگری شدند. مواردی که می‌توانند امنیت رمز عبور را نقض کنند مطابق شکل ۱ دسته‌بندی شده و برای هر مورد پرسش(های) مناسب در نظر گرفته شد.

بعد از بازنگری ادبی پرسش‌نامه توسط یک ویراستار ادبی، پرسش‌نامه به تعدادی از دانشجویان دکترا، نشان‌داده شد، با برخی از کارشناسان ذیربط تلفنی صحبت شد و در یک مورد، پرسش‌نامه کاملاً تکمیل شد. در نهایت نظرات به‌دست آمده از این مرحله بررسی و اعمال شد. بنابراین روایی محتوایی پرسش‌نامه مورد تأیید متخصصان بوده است. برای سنجش پایایی از روش الفای کرونباخ استفاده شد و مقدار ۰,۸۳ به دست آمد.در بازنگری مقاله، یک رفتار جدید «استفاده از رمزهای عبور مشابه» اضافه شد و پرشس‌نامه‌ای روی رفتارهای «استفاده از رمزهای عبور یکسان» و «استفاده از رمزهای عبور مشابه» تدوین شد که مقدار آلفای آن، ۰/۹۵۷ به دست آمد.

در مرحله دوم، یک مطالعه مقدماتی روی پرسش‌نامه انجام شد و پرسش‌ها اصلاح شدند. در نهایت در مرحله سوم پرسش‌نامه پخش شد. جامعه آماری این پژوهش شامل دانشجویان مشغول به تحصیل

در دانشگاه‌های شهرکرد شامل دانشگاه دولتی، دانشگاه پیام نور، آموزشکده فنی دختران و دانشگاه آزاد واقع در شهرکرد است.
نمونه و روش نمونه‌گیری در پژوهش حاضر به این صورت بود که در ابتدا نمونه‌هایی از دانشجویان به شیوه در دسترس در سال ۹۹ انتخاب و به پرسش‌نامه‌ها پاسخ دادند. تعداد ۱۸ پرسش‌نامه به دلیل بی‌دقتی و ناقص‌بودن حذف شدند. در نهایت ۴۴۵ نمونه جمع‌آوری شد. در بازنگری مقاله، نیز تعداد ۸۴ نمونه جدید جمع‌آوری شد. جهت رعایت اخلاق پژوهشی تمامی پاسخ‌دهندگان آگاه شدند که این اطلاعات به منظور اهداف پژوهشی جمع‌آوری می‌شود همچنین پاسخ‌دهندگان با رضایت آگاهانه به پرسش‌نامه‌ها پاسخ دادند و در مورد پنهان ماندن هویت آن‌ها اطمینان داده شد. در مرحله چهارم به منظور آماده سازی داده‌ها از ابزار مایکروسافت اکسل و SPSS نسخه ۱۶ استفاده شد و.
در نهایت جهت تحلیل داده‌های حاصل از پژوهش اطلاعات در دو سطح توصیفی شامل میانگین و انحراف استاندارد و استنباطی شامل ضریب همبستگی اسپیرمن، آزمون تی، تحلیل واریانس، رگرسیون چندگانه به روش گام به گام از ابزار SPSS استفاده شد.

۴. نتایج

در ادامه ابتدا یافته‌های توصیفی و سپس یافته‌های استنباطی پژوهش بیان می‌شوند.

۱.۴.توصیف جامعه نمونه

اطلاعات توصیفی افراد نمونه درجدول ۱ نشان داده شده است. همان‌طورکه مشاهده می شود نیمی از افراد یعنی حدود ۴۰٪ آن‌ها بین ۱۸ تا ۲۰ سال بودند و حدود ۳۵٪ آن‌ها بین ۲۱ و ۲۳ سال بودند که میزان تحصیلات حدود ۸۰٪ آن‌ها کارشناسی بوده است. و عمدتاً جوانان زیر ۲۴ سال مدنظر بوده‌اند. حدود ۷۰٪ افراد زن بودند. کاربران در ۱۰ گروه از رشته‌های تحصیلی مختلف ادبیات و علوم انسانی، فنی و مهندسی، منابع طبیعی و علوم زمین، علوم ریاضی، هنر شامل نقشه‌کشی معماری و طراحی دوخت، دامپزشکی، کشاورزی، علوم پایه، حسابداری و بازرگانی و کامپیوتر و فن‌آوری اطلاعات شاغل بودند. بنابراین جامعه‌ی آماری نماینده انواع مختلف رشته‌های تحصیلی در دانشگاه است. شاخص‌های توصیفی متغیرهای شخصیت در جدول ۲ ارائه شده است. چولگی و کشیدگی متغیرهای شخصیت نیز محاسبه شد که در بازه ۲- و ۲ قرار داشت و نشان‌دهنده نرمال بودن این متغیرها است. برای بررسی متغیر میزان تحصیلات از تحلیل پیرسون استفاده گردید و برای بررسی متغیر جنسیت آزمون تی انجام شد. برای بررسی عامل‌های شخصیت از تحلیل پیرسون و رگرسیون استفاده شد.

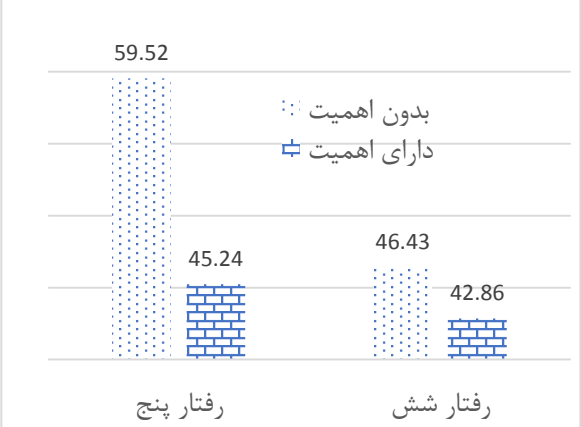
جدول ۲. میانگین و انحراف استاندارد متغیرهای شخصیت پژوهش

	میانگین	انحراف استاندارد
روان‌نژندگرایی (N)	۲۸/۶۴	۹/۹۰
برون‌گرایی (E)	۳۸/۴۰	۹/۴۸
تجربه‌پذیری (O)	۳۵/۸۷	۸/۸۲
توافق‌پذیری (A)	۳۹/۱۸	۸/۶۶
وجدان‌گرایی (C)	۳۷/۵۲	۹/۷۷

اهمیت سایت و موضوع برای صاحب حساب کاربری در تعیین رمز عبور بسیار مؤثر است [۲۱]. به‌طور مثال میانگین میزان استفاده از رمزهای عبور یکسان در سایت‌های مختلف در شکل ۳ نشان داده شده است. همان‌طور که مشاهده می شود میزان نقض امنیت رمز عبور در سیستم‌های بانک، خریدهای الکترونیکی و دانشگاه از سایر سیستم‌ها کمتر بوده است.
منطقی است در سیستم‌هایی که مطالب آن برای دانشجویان مهم نباشد، به امنیت رمز عبور کم‌تر توجه شود. به‌طور مثال درصد

شکل ۳. میانگین میزان استفاده از رمزهای عبور یکسان

افرادی که در سیستم‌های بدون اهمیت از رمز یکسان استفاده کرده‌اند در شکل ۴-رفتار پنج نشان داده شده است. همان‌طور که مشاهده می‌شود در سیستم‌های دارای اهمیت نسبت به سیستم‌های دون اهمیت، افراد بیش‌تری با انتخاب رمزهای یکسان، امنیت رمز عبور را نقض کرده‌اند. همین موضوع در مورد انتخاب رمزهای مشابه کرده‌اند در شکل ۴-رفتار پنج نشان داده شده است. همان‌طور که



شکل ۴. در صد افرادی که با ا ستفاده مجدد از رمزعبور، امنیت رمز را در سیستم‌های دارای اهمیت یا بدون اهمیت نقض کرده‌اند.

در شکل ۴-رفتار پنج مشاهده می‌شود. در سیستم‌های دارای اهمیت، نسبت به سیستم‌های بدون اهمیت، افراد بیش‌تری با انتخاب رمزهای مشابه امنیت رمز عبور را نقض کرده‌اند.

با توجه به این نکته، در ادامه این پژوهش، نقض امنیت رمز عبور در سامانه‌هایی که مطالب آن‌ها برای دانشجویان مهم است، در نظر گرفته شده است.

۲.۴ نقش جنسیت و میزان تحصیلات

نتایج مربوط به تحلیل پیرسون در مورد متغیرهای جنسیت و میزان تحصیلات در جدول ۳ آورده شده است. جدول ۳ نشان می‌دهد که کاربران با میزان تحصیلات بالاتر نسبت به کاربران با میزان تحصیلات پایین‌تر به تعداد دفعات بیش‌تری رمزهای قابل پیش‌بینی

جدول ۳. نتایج آماری در مورد نقش جنسیت و میزان تحصیلات

رفتار	تحصیلات (پیرسون)	زنان (آزمون تی)	مردان
یک	-۰/۰۰۷	۳/۹۸	۳/۹۴
دو	٭۰/۱۱۱	٭٭۰/۰۹	٭٭-۰/۲۱
سه	۰/۰۱۴	٭٭۰/۰۸	٭٭-۰/۲۰
چهار	۰/۰۳۴	۶/۶۸	۶/۹۶
پنج	-۰/۰۵	۴/۱۹	۵۸/۳
شش	-۰/۱۱	۴/۰۶	۳/۵۵
هفت	-۰/۹۴۰	۳/۲۵	۳/۳۹

٭ معنادار در سطح ۰/۰۵ ٭٭ معنادار در سطح ۰/۰۱

انتخاب می‌کنند (رفتار دو). در ضمن نتایج تست تی نشان می‌دهد که در زنان نسبت به مردان، به تعداد دفعات بیش‌تری رمز قابل پیش‌بینی انتخاب شده است (رفتار دو) و همچنین بیش‌تر رمز عبور با دیگران در میان گذاشته شده است (رفتار سه).

۳.۴ نقش عامل‌های شخصیت

نتایج مربوط به تحلیل پیرسون در مورد عامل‌های شخصیت در جدول‌های ۴ آورده شده است. جدول ۴ نشان می‌دهد که متغیر

جدول ۴. ضرایب همبستگی در مورد عامل‌های شخصیت

رفتار	N	E	O	A	C
یک	٭٭۰/۱۵	-۰/۰۵۳	-۰/۰۱۳	-۰/۰۳۱	-۰/۰۳۶
دو	٭۰/۱۲۰	۰/۰۲۶	-۰/۰۵۸	-۰/۰۰۸	-۰/۰۷۷
سه	٭٭۰/۱۶۴	۰/۰۲۸	۰/۰۴۱	۰/۰۰۱	٭۰/۱۰۹
چهار	٭٭۰/۲۸۶	-۰/۰۳۸	٭-۰/۱۱۲	٭-۰/۱۲۱	٭-۰/۲۱۰
پنج	۰/۱۶۶	۰/۰۷۱	-۰/۱۳۲	-۰/۱۶۵	٭-۰/۲۷۹
شش	٭۰/۲۸۶	۰/۰۵۲	۰/۲۱۱	-۰/۱۷۹	٭-۰/۳۴۸
هفت	۰/۰۲۶	-۰/۰۲۰	-۰/۰۰۴	۰-/۰۶۶	-۰/۰۳۱

٭ معنادار در سطح ۰/۰۵ ٭٭ معنادار در سطح ۰/۰۱

روان‌نژندگرایی رابطه مثبت و معنادار با ویژگی نقض امنیت رمز عبور دارند. یعنی افراد با نمرات بالا در روان‌نژندگرایی بیش‌تر از افراد با نمرات پایین در این ویژگی‌ها، رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند. متغیرهای تجربه‌پذیری، توافق‌پذیری و وجدان‌گرایی رابطه منفی و معنادار با نقض امنیت رمز عبور دارند. یعنی افراد با نمرات پایین در تجربه‌پذیری، توافق‌پذیری و وجدان‌گرایی بیش‌تر از افراد با نمرات بالا در این رفتارهای نقض‌کننده امنیت را تکرار کرده‌اند.

جدول ۵. نتایج تحلیل رگرسیون با استفاده از متغیرهای شخصیت

رفتار	R	R^2	متغیر	β	p
یک	۰/۱۴۶	۰/۰۲۱	N	۰/۰۱۶	۰/۰۰۳
دو	۰/۱۱۷	۰/۰۱۴	N	۰/۱۱۷	۰/۰۲۲
سه	۰/۲۰۵	۰/۰۴۲	N	۰/۱۷۴	۰/۰۰۱
			C	۰/۱۲۸	۰/۰۱۴
چهار	۰/۳۵۲	۰/۱۲۴	N	۰/۲۸۳	۰/۰۰۰
			C	-۰/۲۰۳	۰/۰۰۰
پنج	۰/۲۷۹	۰/۰۷۸	C	-۰/۲۷۹	۰/۰۱۰

شش	۰/۳۴۸	۰/۱۲۱	C	-۰/۳۴۸	۰/۰۰۱
هفت	-	-	-	-	-

برای متغیرهای شخصیت تحلیل رگرسیون گام به گام نیز انجام شد. نتایج مربوط به این تحلیل در مورد در جدول ۵ آورده شده است:

نتایج تحلیل رگرسیون جدول ۵ نشان می‌دهد که:

-دانشجویان با نمرات پایین‌تر در این ویژگی، بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند.

-روان‌نژندگرایی در بیش‌تر رابطه‌های رگرسیونی مشاهده شده است و در همه موارد رابطه مثبت با نقض امنیت رمز عبور داشته است: دانشجویان با نمرات بالاتر در تجربه‌پذیری نسبت به دانشجویان با نمرات پایین‌تر در این ویژگی، بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند.

-وجدان‌گرایی نیز در بیش‌تر رابطه‌های رگرسیونی مشاهده شده ولی جهت تأثیر این رابطه در پژوهش ما دوگانه است. نمرات بالای وجدان‌گرایی با تکرار بی‌دقتی در ورود رمز عبور، امنیت رمز عبور را نقض کرده‌اند (رفتار دو) و در همان حال با عدم اشتراک‌گذاری رمز عبور (نفی رفتار سه) و عدم استفاده مجدد از آن (نفی رفتار پنج و نفی رفتار شش)، امنیت آن‌را حفظ کرده‌اند.

۴.۴ نقش رشته تحصیلی

در نهایت به منظور بررسی متغیر رشته تحصیلی با استفاده از تست آنوا، میزان تکرار رفتارهای نقض‌کننده امنیت در کاربران رشته‌های تحصیلی مختلف مقایسه شد. در جدول ۶ نتایج تست آنوا نشان داده شده است.

همان‌طور که در جدول ۶ مشاهده می‌شود، کاربران رشته‌های تحصیلی مختلف در میزان تکرار رفتارهای سه و چهار با هم فرق دارند. نتایج آزمون تعقیبی نشان داد که: - در کاربران رشته‌های

جدول ۶. نتایج تست آنوا برای میزان تکرار رفتارهای نقض‌کننده امنیت رمزعبور در رشته‌های تحصیلی مختلف

	یک	دو	سه	چهار	پنج	شش	هفت
ادبیات و علوم انسانی	-۰/۲۳۹	-۰/۱۵۹	-۰/۱۷۷	۶/۳۴	۴/۲۲	۴/۵۲	۳/۵۶
فنی و مهندسی	-۰/۸۶۱	-۰/۲۴۲	۰/۱۲۶	۶/۸۰	۴	۴/۰۱	۳/۲۲
منابع طبیعی و علوم زمین	-۰/۳۳۵	۰/۰۳۶	۰/۳۱۴	۷/۱۰			۳/۶۵
علوم ریاضی	۰/۱۰۳		۰/۶۲۹	۶/۶۰	۳/۶۱	۳/۸۳	۲/۸۵
هنر	۱/۲۰۸	۱/۲۶	۰/۰۹۲	۶/۵۳			۳/۰۳
علوم پایه	۰/۲۶۸	۰/۲۰۴	-۰/۱۶۰	۷/۹۳	۲/۳۶	۲/۰۷	۲/۶۲
دامپزشکی	۰/۰۸۱	۰/۰۸۳	-۰/۵۲۰	۶/۵۰	۲/۲۵	۲/۳۲	۳/۴۷
کشاورزی	۰/۱۱۰	۱/۳۵	-۰/۰۴۰	۵/۹۶	۴/۳۸	۴/۴۲	۳/۶۴
حسابداری	۰/۲۵۶	۰/۵۶۹	۰/۴۹۵	۸/۱۲			۳/۷۱
کامپیوتر	۰/۱۹۶	۰/۰۰۲	۰/۴۹۵	۶/۹۶			۳/۰۳
معنی‌داری	۰/۱۷۹	۰/۱۵۴	۰/۰۰۰	۰/۰۰۰	۰/۱۸۶	۰/۱	۰/۱

تحصیلی علوم ریاضی نسبت به کاربران رشته‌های تحصیلی فنی و ، مهندسی، منابع طبیعی و علوم زمین، هنر، علوم پایه و کشاورزی، رمز عبور خود را با دیگران در میان گذاشته‌اند (رفتار سه).

-کاربران رشته حسابداری به‌صورت معنی‌داری بیش‌تر از کاربران رشته‌های کشاورزی و ادبیات و علوم انسانی در ورود رمز عبور بی‌دقتی کرده‌اند (رفتار چهار).

۵. بحث و نتیجه‌گیری

همان‌گونه که اشاره شد، هدف از انجام این پژوهش بررسی رابطه بین جنسیت و رشته‌ی تحصیلی، میزان تحصیلات و شخصیت با میزان تکرار رفتارهای ناامن در خصوص رمز عبور است. یافته‌ها در جدول ۷ خلاصه شده است:

در خصوص جنسیت، یافته پژوهش حاضر این است که زنان نسبت به مردان، با انتخاب رمز قابل پیش‌بینی و به اشتراک‌گذاری رمز عبور، امنیت رمز عبور بیش‌تر نقض کرده‌اند. به‌عبارت دیگر کاربران مرد نسبت به کاربران زن؛ کم‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند. برتری مردان نسبت به زنان در مورد امنیت رمز عبور،

در پژوهش‌های قبلی [۷-۸] نیز تأیید شده است. همچنین یافته‌ها هم‌سو با پژوهش‌های جدیدتر در این زمینه است. از جمله پژوهش‌گران در مطالعه [۲۱] نیز دریافته‌اند زنان نسبت به مردان رفتارهای امنیت رمز عبورشان در سطح پایین‌تری قرار دارند.

تبیین احتمالی این نتیجه این‌طور می‌تواند باشد که زنان دانش و تجربی فنی کم‌تری نسبت به مردان دارند [۸]. یکی از موارد دیگر برای توضیح این اختلاف ممکن است تفاوت هنجارهای اجتماعیباشد. چون مردان جهت حفظ امنیت افراد دیگر اقدامات امنیتی را انجام می‌دهند و از نظر رفتار را تبیین کرد. روان شنا سی تکاملی رویکردی در علوم اجتماعی و طبیعی است که به بررسی صفات روانی نظیر حافظه، ادراک و زبان از طریق چشم‌اندازهای تکاملی در رابطه با رفتارهای روان‌شناختی انسان‌ها دارد. یکی از این تبیین‌ها در مورد این که مردان رفتارهای امنیت رمز عبورشان در سطح بالاتری قرار دارد، این است که از ابتدا وظیفه تأمین امنیت خانواده به‌عهده مردان است و مردان نسبت به امنیت حساس‌ترند و زنان هم امنیت و حفظ آن‌را وظیفه دیگران می‌دانند و خیلی به آن حساس نیستند. همچنین در رابطه با میزان تحصیلات نتایج نشانگر این بود که کاربران دارای تحصیلات بالاتر نسبت به تحصیلات پایین‌تر از به تعداد دفعات بیش‌تری از رمزهای قابل پیش‌بینی ا ستفاده می‌کنند. شاید تعدد کارهای مختلف و نیاز به رمز های عبور بیش‌تر، تکرار رفتار های نقض‌کننده امنیت رمز عبور توسط این افراد توضیح دهد.

در رابطه با متغیرهای شخصیتی هم مطابق یافته‌های پژوهش [۱۴]، یافته‌های پژوهش حاضر نشان داد بین روان‌نژندگرایی و رفتارهای نقض امنیت رمز عبور رابطه مثبت وجود دارد. تکانش‌وری و دستپاچه بودن و یا به عبارت دیگر تأملی‌نبودن جزء ویژگی‌هایی

.جدول ۷. جواب سؤال‌های پژوهش

سوال پژوهش		جواب سوال پژوهش	
سوال اول	آیا جنسیت کاربر ایرانی بر میزان استفاده از رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟	بله	زنان نسبت به مردان بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند.
سوال دوم	آیا میزان تحصیلات کاربر ایرانی بر میزان تکرار رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟	بله	یافته‌های پژوهش نشان داد کاربران ایرانی دارای تحصیلات بالاتر نسبت به کاربران با تحصیلات پایین‌تر بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند.
سوال سوم	آیا رشته تحصیلی کاربر ایرانی بر میزان تکرار رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟	بله	کاربران ایرانی در رشته‌های حسابداری و علوم ریاضی نسبت به کاربران سایر رشته‌های تحصیلی بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند.
سوال چهارم	آیا پنج عامل اصلی شخصیت کاربر ایرانی بر میزان تکرار رفتارهای نقض‌کننده امنیت رمز عبور توسط وی تأثیر دارد؟	بله	روان‌نژندی (رابطه مستقیم): کاربران ایرانی روان‌نژند نسبت به کاربران دارای ثبات عاطفی بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند. تجربه‌پذیری (رابطه معکوس): کاربران ایرانی که نسبت به تجربه‌های جدید بسته بوده‌اند، نسبت به تجربه‌پذیر بیش‌تر رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند. توافق‌پذیری (رابطه معکوس): کاربران ایرانی توافق ناپذیر نسبت به کاربران توافق‌پذیر بیش‌تر، رفتارهای نقض‌کننده امنیت رمز عبور را تکرار کرده‌اند. وجدان‌گرایی (رابطه دوگونه): در بعضی شرایط کابران وجدان‌گرا امنیت رمز عبور را نقض کرده‌اند و در بعضی شرایط آن‌را حفظ کرده‌اند.

هستند که عامل روان‌نژندگرایی را با رفتارهای نقض‌کننده امنیت رمز عبور مرتبط می‌سازند.

در ضمن یافته‌ی دیگر این بود که متغیر تجربه‌پذیری رابطه منفی و معنادار با نقض امنیت رمز عبور دارد. یافته‌های پژوهش حاضر در رابطه با عامل تجربه‌پذیری هم‌سو با یافته‌های پژوهش [۱۵] است که در یا فت افراد با تجر به پذیری بالا، امنیت رمز عبور بهتری و آسیب پذیری کم‌تری در برابر دزدی سایبری دارند. یافته‌های پژوهش حاضر ناهم‌سو با نتایج مطالعه [۱۴] است که دریافته‌اند

افراد با نمره بالای تجر به پذیری، معمولاً اطلا عات بیش‌تری در فیسبوک به اشتراک گذاشته و تنظیمات حریم خصوصی باز بیش‌تری دارند که می‌تواند آن‌ها را به حملات، آسیب‌پذیرتر کند.

تبیین رابطه مثبت بین تجربه‌پذیری و رفتارهای نقض امنیت رمز عبور داشتن ویژگی‌هایی مثل اهمیت ارزش‌ها و عقاید برای افرادی با تجربه‌پذیری بالا باشد، با وجودی که افراد تجربه‌پذیر به‌دلیل انعطاف‌پذیری بیش‌تر و حریم خصوصی بازتری دارند، ولی احتمالاً اهمیت به ارزش و عقاید در این‌جا مانع بروز این ویژگی شده است.

در این پژوهش بین توافق‌پذیری و رفتارهای نقض‌کننده امنیت رمز عبور رابطه منفی یافت شد. در مورد عامل توافق‌پذیری و ارتباط منفی آن با رفتارهای نقض امنیت رمز عبور علل متفاوتی ممکن است مطرح باشد، از جمله گرایش به اعتدال و باحوصله بودن می‌تواند به آن‌ها در حفظ و نگه‌داری رمز عبور کمک کننده باشد.

ولی جهت تأثیر این رابطه با وجدان‌گرایی دو گونه است. نمرات بالای وجدان‌گرایی با بی‌دقتی در ورود رمز عبور، امنیت رمز عبور را نقض کرده‌اند و در همان حال با عدم به اشتراک‌گذاری رمز عبور و عدم استفاده مجدد از آن، امنیت آن را حفظ کرده‌اند. یافته‌های پژوهش حاضر هم‌سو با نتایج مطالعه [۱۲] است که رابطه مثبت بین دو عامل وجدان‌گرایی با رفتارهای حفظ امنیت مربوط به تکنولوژی اطلاعات گزارش کرده‌اند.

از تبیین‌های احتمالی این رابطه می‌توان این باشد که عامل وجدان‌گرایی با صفت وظیفه‌شناسی ارتباط دارد و می‌تواند تبیین‌کننده رابطه منفی بین عامل وجدان‌گرایی و رفتار عدم اشتراک‌گذاری رمز عبور باشد. زیرا افراد وظیفه‌شناس احتمالاً دقت بیش‌تری در حفظ و مراقبت از رمزهای عبور خود دارند و یا ممکن است به علت داشتن ویژگی نظم و ترتیب در افراد وجدان‌گرا باشند، منتها ممکن است به خاطر ویژگی اختصاص زمان به پدیده‌های مختلف و ایجاد اضافه بار شناختی برای خودشان موقع ورود رمز عبور دقت چندانی نداشته باشند.

در ضمن یافته‌های حاصل از پژوهش نشان می‌دهد بین وجدان‌گرایی و استفاده از رمزهای مشابه و یکسان رابطه معکوسی وجود دارد. به عبارت دیگر افراد وجدان‌گراتر به میزان کم‌تری از رمزهای مشابه و تکراری استفاده می‌کنند. تبیین این یافته می‌تواند این‌گونه باشد که وجدان‌گرایی با صفاتی مثل احتیاط ارتباط دارد و افراد محتاط به نسبت افراد غیر محتاط احتمال این‌که رمزهای تکراری و مشابه به کار ببرند، کم‌تر است. در ضمن افراد وجدان‌گرا، وظیفه‌شناس‌تر هستند و این موضوع هم احتمال استفاده از رمزهای تکراری و مشابه را کم‌تر می‌کند. در ضمن ویژگی منظم بودن در افراد وجدان‌گرا باعث می شود در انتخاب رمزها ، دقت و نظم بیش‌تری داشته باشند و رمزهای قبلی خود را کم‌تر مورد استفاده قرار دهند.

در مورد رشته‌های تحصیلی یافته این پژوهش در مورد ضعف کاربران رشته‌های، علوم ریاضی و حسابداری ناهم‌سو با یافته‌های پژوهش [۱۱] است. احتمالاً این نتیجه در سال ۲۰۱۲ به دلیل تجربه فناوری کم‌تر رشته‌های تحصیلی هنرهای آزاد به‌دست آمده است. امروزه همه رشته‌های تحصیلی اطلاعات لازم را در خصوص رمز عبور دارند. لیکن رشته‌های وابسته به اعداد ممکن است حافظه خوبی برای نگهداری رمزهای عبور نداشته و از یک رمز یکسان در کاربردهای مختلف استفاده کنند یا رمز خود را به شکل‌هایی ذخیره و به اشتراک بگذارند.

در این پژوهش، محدودیت‌های چندی وجود داشت. از جمله این که جامعه‌ی آماری محدود به دانشجویان است. ممکن است تکرار پژوهش در جامعه‌های غیردانشجویی به نتایج متفاوتی منجر شود. البته در این‌جا با پخش تعداد زیاد پرسش‌نامه در دانشگاه‌های مختلف و در بین رشته‌های مختلف و مقاطع مختلف، سعی شد این محدودیت کم‌رنگ شود. در ضمن نتایج با تحلیل همبستگی به‌دست آمده است. تحلیل همبستگی نشان‌دهنده‌ی دلیل رابطه علت و معلولی نیست.

این پژوهش پیشنهادات چندی را برای محققان ارائه کرده است. پیشنهاد می‌شود پژوهش را در جامعه‌ی آماری بزرگ‌تر و غیردانشجویی تکرار گردد. می‌توان جنبه‌های دیگری از امنیت را مدنظر قرار داد. به‌طور مثال رفتارهای تفاوت‌های افراد در مورد نصب آنتی‌ویروس و خرید اینترنتی بررسی کرد. می‌توان رفتارهای امنیتی افراد را به صورت‌های خودکار و از بانک‌های سامانه‌ها جمع‌آوری کرد. با استفاده از این نتایج می‌توان دانشجویان را در زمینه انتخاب رمز عبور آموزش داد. یافته‌های پژوهش حاضر با در نظر گرفتن تفاوت فردی در رابطه با جنسیت، شخصیت و رشته در زمینه رفتارها و ادراکات امنیتی، به حوزه امنیت اطلاعات رفتاری کمک می‌کند. همچنین نتایج ممکن است از اهمیت ویژه‌ای در هنگام شناسایی رفتارهای مشکوک [۲۲]، طراحی آموزش امنیتی، و آگاهی بخشی دانشجویان به‌عنوان گروهی از مهم‌ترین آینده‌سازان جامعه برخوردار باشد.

مراجع

[۱] اسدالله شاه بهرامی، رامین رفیع زاده کاسانی، حسین پوریوسفی درگاه، "شناسایی و اولویت‌بندی پارامترهای تاثیرگذار بر سیستم مدیریت امنیت اطلاعات (مطالعه موردی: شعب تامین‌اجتماعی استان گیلان)"، *دوفصلنامه اطلاعات و ارتباطات ایران*، دوره ۱۰، شماره ۳۵؛ صفحات ۵۷-۷۴، ۱۳۹۷.

[۲] M. A. Sasse, S. Brostoff, & D, Weirich. "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security". BT technology journal. vol. ۱۹, no. ۳, pp. ۱۲۲-۱۳۱, ۲۰۰۱.

[۳] C. Anschuetz, "The Weakest Link Is Your Strongest Security Asset. Retrieved from". http://blogs.wsj.com/cio/۲۰۱۵/۰۲/۲۶/the-weakest-link-is-your-strongest-securityasset/

[۴] J. Leach. "Improving user security behaviour". Computers & Security. vol.۲۲, no. ۸, pp. ۶۸۵- ۶۹۲, ۲۰۰۱.

[۵] A. Kovačević, N. Putnik, & O. Tošković. "Factors Related to Cyber Security Behavior". IEEE Access, vol. ۸, ۲۰۲۰. ۱۲۵۱۴۰-۱۲۵۱۴۸.

[۶] J. Blythe, J. Camp, & V. Garg. "Targeted risk communication for computer security". Proceedings of the ۱۶th International Conference on Intelligent User Interfaces - IUI '۱۱, pp. ۲۹۵-۲۹۸, ۲۰۱۱.

[۷] R. Shay, S. Komanduri, P. G, Kelley, P. G., Leon, M. L. Mazurek, L., Bauer, L. F. Cranor."Encountering stronger password requirements". Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '۱۰, ۲. ۲۰۱۰.

[۸] S. Sheng, M. Holbrook, P. Kumaraguru, L. F Cranor, & J. Downs, "Who falls for phish?" Proceedings of the ۲۸th International Conference on Human Factors in Computing Systems - CHI '۱۰, pp. ۳۷۳-۳۸۲, ۲۰۱۰.

[۹] Jr. JL. Parrish, J.L. Bailey, & J.F. Courtney. "A personality based model for determining susceptibility to phishing attacks." Little Rock: University of Arkansas, pp. ۲۸۵-۲۹۶, ۲۰۰۹.

[۱۰] J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, & A. Darwish. "Phishing in a university community: Two large scale phishing experiments". International Conference on Innovations in Information Technology (IIT), pp. ۲۴۹-۲۵۴, ۲۰۱۲.

[۱۱] A. Darwish, A.E. Zarka ۷ F. Aloul. "Towards understanding phishing victims' profile". International Conference on Computer Systems and Industrial Informatics. IEEE, ۲۰۱۲.

[۱۲] J. Shropshire, M. Warkentin, A. Johnston, & M. Schmidt. "Personality and IT security: An application of the five-factor model". AMCIS ۲۰۰۶ Proceedings. pp.۴۱۵, ۲۰۰۶.

[۱۳] A. Maraj, M. V. Martin, M. Shane, M. and Mannan. "On the Null Relationship between Personality Types and Passwords". Conference on Privacy, Security and Trust. Fredericton, NB, Canada. ۲۰۱۹.

[۱۴] T. Halevi, J. Lewis, & N. Memon. "A pilot study of cyber security and privacy related behavior and personality traits". Proceedings of the ۲۲nd International Conference on World Wide Web - WWW '۱۳ Companion, pp. ۷۳۷-۷۴۴, ۲۰۱۳.

[۱۵] M. Pattinson, C. Jerram, K. Parsons, A. Mccormac, & M. Butavicius. "Why do some people manage phishing e- mails better than others?" Info Mngmnt & Comp Security Information Management & Computer Security, vol. ۲۰, no. ۱, pp.۱۸-۲۸, ۲۰۱۲.

[۱۶] S. Egelman, & E. Peer. "Predicting privacy and security attitudes". SIGCAS Comput. Soc. ACM SIGCAS Computers and Society, vol. ۴۵, no.۱, pp. ۲۲-۲۸, ۲۰۱۵.

[۱۷] M, Zviran & WJ. Haga, " Password security: an empirical study". Journal of Management Information Systems. vol. ۱۵, no. ۴, pp. ۱۶۱-۸۵, ۱۹۹۹.

[۱۸] تقی گروسی‌فرشی، نعمت الله تقوی، "رویکردی نوین در ارزیابی شخصیت (کاربرد تحلیل عاملی در مطالعات شخصیت)"، انتشارات جامعه پژوه، دانیال، ۱۳۸۰.

[۱۹] فرهاد خرمایی، اعظم فرمانی، "بررسی شاخص های روانسنجی فرم کوتاه پرسشنامه پنج عامل بزرگ شخصیت"، روشها و مدلهای روان شناختی، دوره ۴، شماره ۱۶، صفحات ۲۹-۳۹، ۱۳۹۳.

[۲۰] S. Brandi. "An Empirical Assessment of User Online Security Behavior: Evidence from a University". Diss. U. of Maryland Libraries, ۲۰۱۶.

[۲۱] S. Pearman, J. Thomas, P.E. Naeini, H. Habib, L. Bauer, N. Christin, … & A. Forget. "Let's go in for a closer look: Observing passwords in their natural habitat". In Proceedings of the ۲۰۱۷ ACM SIGSAC Conference on Computer and Communications Security, pp. ۲۹۵-۳۱۰, ۲۰۱۷

[۲۲] لیلا ساروخانی، غلامعلی منتظر، "طراحی و پیاده سازی سیستم هوشمند شناسایی رفتار مشکوک در بانکداری اینترنتی به کمک نظریه مجموعه های فازی"، دوفصلنامه فناوری اطلاعات و ارتباطات ایران، دوره ۱، شماره ۱، ۱۳۹۲.