شاپا چاپی: ۱۸۴۱ - ۲۷۸۳
شاپا الکترونیکی: ۱۹۲۲-۲۷۸۳

تمدن حقوقی

دوره ۵ – شماره۱۲ – پاییز ۱۴۰۱

Legal Civilization
Vol. 5, No. 12, Autumn 2022
Pages: 345-362
Article Type: Original Research
http://www.pzhfars.ir/article_155244.html
doi: 10.22034/LC.2022.155244

تمدن حقوقی
دوره ۵، شماره ۱۲، پاییز ۱۴۰۱
صفحات: ۳۶۲-۳۴۵
نوع مقاله: علمی پژوهشی

Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic with an Approach to Routine Activity Theory

Maryam Kamaei
PhD Student in Criminal Law and Criminology, Lecturer at Khuzestan University of Applied Sciences, Ahvaz, Iran

بررسی تغییر از جرائم خیابانی به جرائم سایبری در آغاز همه‌گیری کووید-۱۹ رویکردی به نظریه فعالیت‌های روزانه

مریم کمائی
دانشجوی دکتری حقوق جزا و جرم‌شناسی، مدرس دانشگاه علمی کاربردی واحد فرماندهی انتظامی استان خوزستان، اهواز، ایران
maryamkamaei2019@gmail.com
http://orcid.org/0000-0003-0483-4566

Abstract

Covid-19 virus has made an impact on virtually every aspect of our lives. The current study utilizes secondary data to identify patterns and trends related to shifting crime from the physical to the cyber domain thatfor finding new ways to commit crimes. Research findings show that while many crimes such as theft, rape and murder have decreased at the beginning of the pandemic, we have seen an increase in cyber crimes, vehicle theft and domestic violence. The current study looks specifically at phishing and what new trends are observed due to Covid-19. The current research based on routine activity theory and shows its connection with physical space and cyberspace. The implications of our work can be used by scholars who want to continue researching this new phenomenon. Developing new phishing training and awareness programs should be focused around possible scenarios involving COVID-19. Studies show that victims are more likely to fall prey to them during times of fear and uncertainty such as the current pandemic.

Keywords: Internet, Cybercrime, Phishing, Covid-19 Virus, Routine Activity Theory.

چکیده

ویروس کووید-۱۹ تقریباً بر تمام جنبه‌های زندگی ما تأثیر گذاشته است. پژوهش حاضر از داده‌های ثانویه برای شناسایی الگوها و روندهای مرتبط با تغییر جرم از حوزه فیزیکی به حوزه سایبری استفاده می‌کند که به دنبال راه‌های جدیدی برای ارتکاب جنایت هستند. یافته‌های پژوهش نشان می‌دهد که درحالی‌که بسیاری از جرائم مانند سرقت، تجاوز و قتل در ابتدای همه‌گیری کاهش یافته است شاهد افزایش جرائم سایبری، سرقت وسایل نقلیه و خشونت خانگی هستیم. مطالعه فعلی به طور خاص به فیشینگ و روندهای جدیدی که به دلیل کووید-۱۹ مشاهده می‌شود، می‌پردازد. این پژوهش مبتنی‌بر نظریه فعالیت‌های روزانه است و ارتباط آن را با فضای فیزیکی و فضای مجازی نشان می‌دهد. مفاهیم این مقاله می‌تواند توسط محققانی که می‌خواهند به تحقیق در مورد این پدیده جدید ادامه دهند، استفاده شود. توسعه آموزش فیشینگ جدید و برنامه‌های آگاهی‌دهنده باید حول سناریوهای احتمالی مرتبط با کووید-۱۹ متمرکز شود. مطالعات نشان می‌دهد که قربانیان بیشتر در مواقع ترس و عدم اطمینان مانند همه‌گیری کنونی طعمه آن‌ها می‌شوند.

واژگان کلیدی: اینترنت، جرائم سایبری، فیشینگ، ویروس کووید-۱۹، تئوری فعالیت‌های روزانه.

Received: 2022/08/13 - Review: 2022/09/20 - Accepted: 2022/10/08

دریافت مقاله: ۱۴۰۱/۰۵/۲۲ بازنگری مقاله: ۱۴۰۱/۰۶/۲۹ - پذیرش مقاله: ۱۴۰۱/۰۷/۱۶

ارجاع:
کمائی، مریم؛ (۱۴۰۱)، بررسی تغییر از جرائم خیابانی به جرائم سایبری در آغاز همه‌گیری کووید-۱۹ رویکردی به نظریه فعالیت‌های روزانه، تمدن حقوقی، شماره ۱۲.

مقدمه

جرائم سایبری در دهه گذشته رو به افزایش بوده است. طبق گزارش[1] اکسنتور[2]، میانگین تعداد نقض‌های امنیتی در سال ۲۰۱۸ با یازده درصد افزایش از یکصد و سی به یکصد و چهل و پنج افزایش یافته است و میانگین هزینه جرائم سایبری برای یک سازمان ۱. ۴ میلیون دلار به ۱۳. ۰ میلیون دلار افزایش یافته است. نویسندگان تخمین می‌زنند که هزینه‌های جهانی جرائم سایبری طی پنج سال آینده به ۵. ۲ تریلیون دلار خواهد رسید. این افزایش قابل‌توجهی در مقایسه با سال ۲۰۱۳ است که کونرانت[3] و همکاران (۲۰۱۶) برآورد کرد که هزینه جهانی جرائم سایبری چهارصد و چهل و پنج میلیارد دلار است. بیشتر خسارات مالی ناشی از حساب‌های سرقت شده و شماره‌های کارت اعتباری سرقت شده است که اغلب با حملات فیشینگ به دست می‌آید.

فیشینگ نوعی از جرائم سایبری است که در آن مهاجمان ایمیل‌های مخرب را مشروع جلوه می‌دهند. هدف سرقت اطلاعات کاربری، کارت اعتباری و سایر اطلاعات شخصی حساس است که می‌تواند منجر به سرقت هویت، کلاهبرداری و به خطر انداختن دستگاه شود (Kirda & Kruegel,2006). ایمیل‌های فیشینگ مهندسی اجتماعی و تکنیک‌های جعل را ترکیب می‌کنند تا افراد را متقاعد کنند که اطلاعات

1- https: //www. accenture. com/us-en/insights/security/cost-cybercrime-study, accessed on April 9, 2021
2- Accenture
3- Konradt

خود را ارائه دهند. فعالیت آنلاین مانند بانکداری یا خرید می‌تواند احتمال قربانی‌شدن فیشینگ را افزایش دهد (Reyns,2015).

با توجه به شیوع کووید-۱۹، به میلیون‌ها، اگر نگوییم میلیاردها نفر در سراسر جهان دستور داده‌اند در خانه بمانند و قرنطینه را رعایت کنند. این واقعیت جدید تقریباً بر هر جنبه‌ای از زندگی روزمره ما تأثیر قابل‌توجهی گذاشت. کار در خانه، آموزش آنلاین، خرید، بانکداری، پزشکی از راه دور و غیره به یک امر عادی تبدیل شد. چنین تغییر عمده‌ای در تاریخ جهان بی‌سابقه است و ما را با چالش‌های متعددی مواجه کرده است. یکی از آن‌ها تغییر جرائم فیزیکی به جرائم سایبری است که در مراحل اولیه همه‌گیری مشاهده شد.

براساس تئوری فعالیت روزانه، برای وقوع جرم باید یک مجرم باانگیزه، یک هدف مناسب و فقدان نگهبانی توانا وجود داشته باشد. با این حال، از آن جایی که افراد بسیار کمتری در خیابان‌ها -رفتن به محل کار، مدرسه و رستوران‌ها- حضور دارند، احتمال حمله مجرمان به قربانیان به میزان قابل‌توجهی کاهش یافته است. در شیکاگو، یکی از خشن‌ترین شهرهای آمریکا، دستگیری مواد مخدر در هفته‌هایی که شهر در مارس ۲۰۲۰ تعطیل شد، چهل و دو درصد در مقایسه با مدت مشابه سال گذشته کاهش یافت. میامی به مدت هفت هفته بدون قتل بود که اولین بار از سال ۱۹۵۷[۴] است. درحالی‌که برخی ممکن است این را یک پیروزی و نتیجه مثبت بیماری همه گیر بدانند، تجزیه و تحلیل عمیق‌تر از روند فعلی در جرائم سایبری نشان می‌دهد که مجرمان در حال تغییر وضعیت فیزیکی به حوزه سایبری هستند. در مارس ۲۰۲۰، رییس کمیسیون اروپا، اورسولا فون در لاین، هشدار داد که جرائم سایبری در اتحادیه اروپا به دلیل شیوع ویروس کرونا افزایش یافته است. او تأکید می‌کند که مهاجمان اکنون قربانیان خود را به صورت آنلاین دنبال می‌کنند و حتی با طراحی کمپین‌های فیشینگ براساس نگرانی‌های کووید-۱۹ از همه‌گیری به نفع خود استفاده می‌کنند. این مثال‌ها نشان می‌دهند که چگونه در شروع همه‌گیری، مجرمان بلافاصله شروع به بررسی فرصت‌های جایگزین برای توهین کردند.

افزودن رشد مداوم جرائم سایبری در دهه گذشته به ترس و اضطراب ناشی از کروناویروس، موقعیت منحصر به فردی را ایجاد می‌کند که مجرمان می‌توانند از آن سوءاستفاده کنند. علاوه بر این، کالایی‌شدن جرائم سایبری (Van Wegberg et al. ,2018) این کار را برای افرادی که دارای حداقل مهارت و تجربه هستند، بسیار آسان می‌کند تا فعالیت‌های جرائم سایبری را برون سپاری کند، بنابراین موانع ورود به این

4- https: //www. cbsnews. com/news/miami-no-homicide-seven-weeks/, accessed on April 9, 2021

حوزه را کاهش می‌دهد. حداقل پانزده تا هفده میلیون دلار بین سال‌های ۲۰۱۱ تا ۲۰۱۷ برای کالاهای جرائم سایبری در ایالات متحده آمریکا هزینه شده است. نویسندگان اشاره می‌کنند که چگونه ایمیل‌های فیشینگ یکی از رایج‌ترین کانال‌ها برای توزیع نرم افزارهای مخرب هستند. علاوه بر این، کلاهبرداری‌های فیشینگ به راحتی قابل انجام هستند زیرا به منابع بسیار محدود و مهارت‌های فنی نیاز دارند. مجموعه این عوامل فیشینگ را برای مجرمان باانگیزه بسیار جذاب و پرسود می‌کند. ناتوانی فعلی آن‌ها در ارتکاب جرائم فیزیکی عامل اصلی تغییر از جرائم فیزیکی به جرائم سایبری است.

هدف مطالعه حاضر بررسی تغییر از جرائم فیزیکی به جرائم سایبری در آغاز همه‌گیری کووید-۱۹ است. این یک رویداد تاریخی جهانی بی‌سابقه است و ما هنوز در حال جمع‌آوری داده‌ها برای درک بهتر خود ویروس کرونا و تأثیر گسترده‌تر آن بر جامعه هستیم. ماهیت پویای این بیماری همه گیر چالش‌های منحصر به فردی را به همراه دارد. بنابراین، هدف کار ما روشن‌کردن چگونگی انتقال جرم در ابتدا به فضای مجازی و پیامدهای آن برای سازمان‌ها و افراد است. سؤال پژوهشی که مطالعه را هدایت می‌کند این است: پیامدهای کووید-۱۹ بر جرم در شروع همه‌گیری چیست؟ و فرضیه ما این است که به دلیل قرنطینه گسترده در سراسر جهان در آغاز همه‌گیری، تغییری از جرائم فیزیکی به سایبری رخ داده است.

نگارنده برای پاسخ به سؤال تحقیق و آزمون فرضیه از داده‌های ثانویه استفاده می‌کند. یکی از چالش‌های این مطالعه جدیدبودن موضوع و کمبود منابع علمی موجود در مورد تأثیر کووید-۱۹ بر جرم و جنایت است. بنابراین، نویسنده در حال بررسی انواع مقالات خبری، گزارش‌های دولتی و نشریات بخش خصوصی برای شناسایی روندهای فعلی در جرم و جنایت و بررسی این که آیا تغییرات احتمالی در نحوه وقوع آن در طول یک بیماری همه‌گیر وجود دارد یا خیر. کار ما مبتنی‌بر تئوری فعالیت‌های معمول است زیرا به طور گسترده در زمینه فیزیکی (Tewksbury & Mustaine, 2003) و (Robinson,1999) و (Groff,2007) و قربانی‌شدن جرائم سایبری (Yar, 2005)و(Leukfeldt & Yar, 2016)و(Holt & Bossler, 2008) استفاده شده است.

۱- بررسی ادبیات پژوهش

۱-۱- جرائم سایبری

نگرانی‌های مربوط به امنیت سایبری با اتکای بیشتر به فناوری در زندگی روزمره‌مان افزایش یافته است. به

گفته سارنو و همکاران (۲۰۱۹)، اغلب چنین حملاتی نتیجه کلاهبرداری‌های فیشینگ است که در آن افراد فریب می‌خورند تا روی پیوندهای مخرب در ایمیل‌هایی که جعلی به نظر می‌رسند، کلیک کنند. براساس یک مطالعه که داده‌های سال ۲۰۱۹ را بررسی می‌کند، نود درصد از موارد نقض داده‌ها را فیشینگ تشکیل می‌دهد. هفتادوشش درصد از کسب و کارها گزارش داده‌اند که در سال گذشته قربانی یک حمله فیشینگ شده‌اند و سی درصد از پیام‌های فیشینگ توسط کاربران هدف باز می‌شوند. کلاهبرداری‌های مرتبط با ایمیل تجاری بیش از دوازده میلیارد دلار ضرر داشته است.

این اعداد در زمینه‌سازمان‌های تجاری است که وظایف اختصاصی فناوری اطلاعات و امنیت دارند. علاوه بر این، بیشتر سازمان‌ها نوعی آموزش فیشینگ و آگاهی برای کارکنان ارائه می‌کنند و از سیستم‌های فیلترینگ پیچیده برای مسدودکردن ایمیل‌های مشکوک استفاده می‌کنند. از آن جایی که بسیاری از کارمندان اکنون در خانه کار می‌کنند، چالش‌های بیشتری را برای متخصصان فناوری اطلاعات ایجاد می‌کند تا شبکه‌ها و دستگاه‌های خود را ایمن کنند. فورنل و همکاران در (۲۰۰۷) مطالعه‌ای انجام داد و دریافت که خطر افزایشی برای کاربران خانگی وجود دارد. به‌عنوان مثال، هنگامی که سازمان‌ها دفاع خود را سخت‌تر می‌کنند، سیستم‌های کاربر خانگی به دلیل مکانیسم‌های حفاظتی کمتری که دارند، ناگهان به اهداف جذاب‌تری برای سازش تبدیل می‌شوند. در نتیجه، آن‌ها می‌توانند در بات نت‌ها و حملات انکار سرویس توزیع شده[5] مورد سوءاستفاده قرار گیرند. این مطالعه نشان داد که حتی اگر کاربران به توانایی خود در محافظت از سیستم‌ها و دستگاه‌های خود اطمینان بالایی داشتند، حوزه‌های مختلفی وجود داشت که دانش و درک مطلوبی در آن‌ها وجود نداشت. این مسائل اکنون از شبکه‌های شخصی به شبکه‌های سازمانی و دستگاه‌های ضروری برای دفاتر خانگی در طول همه‌گیری منتقل می‌شوند. بنابراین سطح حمله هر سازمانی افزایش می‌یابد و می‌تواند هدف بالقوه‌ای برای مجرمان باشد.

وقتی صحبت از جرائم سایبری می‌شود، فعالیت‌های سازمان یافته زیادی وجود دارد. چتر جرائم سایبری طیف وسیعی از مهارت‌ها را در بر می‌گیرد از بچه‌های اسکریپتی که دانش کمی دارند و به سوءاستفاده‌های موجود متکی هستند، تا دولت‌هایی که از تهدیدات پایدار پیشرفته[6] استفاده می‌کنند. با این حال، کسانی که دسترسی بیشتری به منابع دارند، بزرگ‌ترین تهدید هستند و معمولاً سندیکاها و

5- DDoS
6- APT

سازمان‌های جنایتکار هستند. جرائم سایبری سازمان‌یافته با حملات فیشینگ (Birk et al. ,2007) تهدیدات امنیت ملی (Grabosky,2015)، حملات سایبری (Jian et al. ,2020)، تروریسم (Shelley,2003) و اقتصاد زیرزمینی (Yip et al. ,2012) مرتبط است. جرائم سایبری در حال حاضر مافیای امروزی حتی قبل از همه‌گیری بود. بنابراین، منطقی است که فرض کنیم سازمان‌های جنایی تلاش‌های خود را روی جرائم سایبری متمرکز خواهند کرد، به‌ویژه در مراحل اولیه همه‌گیری، زمانی که بیشتر وقت خود را در مقابل نمایشگرهای خود می‌گذرانند و نه در خیابان.

۲-۱- فیشینگ

وقتی صحبت از فیشینگ به میان می‌آید، درحالی‌که تعریف جهانی وجود ندارد که همه محققان با آن موافق باشند، بسیاری از تعاریف موجود مفاهیم اولیه یکسانی را پوشش می‌دهند. کردا و کرودل در (۲۰۰۶) بر جنبه مالی فیشینگ تمرکز می‌کنند و نگرانی اصلی آن‌ها این است که چگونه می‌توان از سرقت هویت برای دسترسی به حساب‌های بانکی و کارت‌های اعتباری قربانیان استفاده کرد. سارنو و همکاران در (۲۰۱۹) از تعریفی استفاده می‌کند که بیشتر به کلاهبرداری از افراد با هدف سرقت اطلاعات شخصی آن‌ها مربوط می‌شود. آن‌ها همچنین بر شیوه‌های کلاهبرداری اعمال شده توسط فیشرها برای طعمه زدن کاربران برای کلیک‌کردن روی پیوندهای موجود در ایمیل‌ها تأکید می‌کنند.

فقدان یک تعریف توافقی از فیشینگ توسط لست ریجر در (۲۰۱۴) مورد بررسی قرار گرفت که یک مرور ادبیات سیستماتیک از نشریات بررسی شده انجام داد. تعریف اجماع پیشنهادی چندین جنبه مهم مانند مقیاس‌پذیری، فریب، جعل هویت و هدف را در بر می‌گیرد. این مطالعه بسیاری از نظریه‌های جرم‌شناسی مانند نظریه فعالیت‌های معمول، نظریه انتخاب عقلانی و نظریه الگوی جرم را در بر گرفت. تازگی در این مطالعه مربوط به مشاهده فیشینگ به‌عنوان یک جرم مقیاس پذیر است. این به دلیل این ایده است که یک ایمیل فیشینگ می‌تواند با تلاش بسیار کمی برای یک یا هزاران نفر مختلف ارسال شود. چنین رویکردی با جرائم فیزیکی بسیار متفاوت است و می‌تواند به مزایای بسیار بزرگ‌تری منجر شود و در عین حال خطر را برای مهاجمان کاهش دهد. با توجه به افزایش کلی کلاهبرداری‌های فیشینگ، درک بهتر مشخصات قربانی مهم است، بنابراین می‌توانیم آگاهی و آموزش بیشتری برای جلوگیری از حملات بعدی ارائه دهیم. فناوری نقش مهمی را به‌عنوان مکانیزمی برای مسدودکردن ایمیل‌های مشکوک ایفا می‌کند، اما مطالعات نشان داده‌اند که انسان‌ها حلقه ضعیف هستند (Laszka et al. ,2013) و هر برنامه

پیشگیری باید به جای ابزارهای خودکار، آن‌ها را هدف قرار دهد.

۳-۱- جرائم سایبری در مقابل جرائم فیزیکی

جرائم سایبری و جرائم فیزیکی دارای برخی ویژگی‌های مشترک هستند. به‌عنوان مثال، لوستوس در (۲۰۱۳) استدلال می‌کند که جرائم سایبری را می‌توان به همان روش جنایت سنتی سازمان‌دهی کرد. به طور خاص، نویسنده افزایش مجرمان سایبری حرفه‌ای و توسعه گروه‌های آنلاین متعدد را بررسی می‌کند، جایی که این مجرمان سایبری در طرح‌هایی به هم می‌پیوندند. پلتفرم‌های اجتماعی و مکان‌هایی مانند تاریک‌نت ارتباطات خود را بیشتر تسهیل کرده‌اند و به ایجاد سندیکاهای جرائم سایبری کمک کرده‌اند (Wehinger,2011). در مطالعه دیگری، یار در (۲۰۰۵) مقایسه‌ای بین جرائم «مجازی» و «زمینی» براساس تئوری فعالیت‌های روزانه ارائه می‌دهد. این مطالعه میزان انتقال مفاهیم این نظریه را به جرائم ارتکابی در یک محیط مجازی بررسی می‌کند و نتیجه می‌گیرد که اگرچه برخی از مفاهیم اصلی نظریه را می‌توان در جرائم سایبری به کار برد، تفاوت‌های مهمی بین مجازی و زمینی وجود دارد. بنابراین، یار (۲۰۰۵) استدلال می‌کند که جرم سایبری در واقع نمایانگر ظهور شکل جدیدی از جنایت است.

مفهوم فضای مجازی به‌عنوان گسترش فضای فیزیکی توسط تعدادی از مطالعات جدیدتر نیز پشتیبانی شده است. ولن کلانبرگ در (۲۰۱۹) نشان می‌دهد که همپوشانی قابل‌توجهی بین قربانی و مجرم وجود دارد و همبستگی‌هایی مانند کنترل خود پایین وجود دارد. آن‌ها تفاوت‌ها را در قربانی‌سازی، توهین‌کردن و قربانی‌شدن در مورد جرائم سایبری توضیح می‌دهند. علاوه بر این، نویسندگان برخی از جرائم سایبری مرتبط با جرائم دیجیتال و سنتی را پیدا کردند. همپوشانی قربانی و مجرم نشان می‌دهد که بسیاری از قربانیان مجرم هستند و بسیاری از مجرمان قربانی‌شدن را تجربه کرده‌اند (Jennings et al. ,2010). درحالی‌که این موضوع در ابتدا در زمینه جرائم فیزیکی مورد بررسی قرار گرفت، این روند حتی در مورد جرائم سایبری نیز باقی می‌ماند (Marcum et al. ,2014).

یکی از مسائل اصلی جرائم سایبری، ایجاد صلاحیت قضایی است. طبق نظر برنر در (۲۰۰۶)، جرم فیزیکی تقریباً همیشه یک پدیده محلی است زیرا مرتکب و قربانی هر دو در زمان وقوع جرم در مکان و زمان یکسانی هستند. بنابراین جرم قلمرو تلقی می‌شود و محل آن تعیین‌کننده صلاحیت است. وقتی به جرائم سایبری نگاه می‌کنیم، این یک مشکل می‌شود، زیرا آن‌ها از نظر فیزیکی به یک مکان محدود نیستند. قربانی و مجرم حتی می‌توانند از نظر فیزیکی در کشورهای مختلف باشند. در این موارد، حاکمان

مختلف می‌توانند ادعای جنایت‌های مختلفی را داشته باشند. یکی دیگر از عوارض جرائم سایبری این است که برخی کشورها ممکن است معاهدات استرداد نداشته باشند. بنابراین، حتی اگر مجریان قانون بتوانند ثابت کنند که چه کسی مرتکب جرم شده است، ممکن است نتوانند مرتکب را تحت تعقیب قرار دهند و در نهایت، قوانین مربوط به جرائم سایبری هنوز در حال توسعه است، بنابراین اغلب اوقات ممکن است به چالش کشیدن افرادی که مرتکب جرائم سایبری می‌شوند، چالش برانگیز باشد.

کالایی‌شدن جرائم سایبری (Sood & Enbody,2013)و(Van Wegberg et al. ,2018) همراه با ناتوانی در تحقیق و پیگرد قانونی آن‌ها، جرائم سایبری را به یک تجارت پرسود برای مجرمان تبدیل می‌کند. مراحل اولیه واقعیت کووید-۱۹ زمانی که به اکثر مردم دستور داده شد در خانه بمانند، فرصتی منحصر به فرد برای مهاجمان فراهم می‌کند تا به راحتی از حوزه فیزیکی به حوزه سایبری جابجا شوند. منابع متعددی قبلاً افزایش جرائم سایبری را از زمان شروع همه‌گیری گزارش کرده‌اند. به‌عنوان مثال، وزارت امنیت داخلی ایالات متحده آمریکا هشداری را در آوریل ۲۰۲۰[7] صادر کرد و گزارش داد که افزایش یکصد و بیست و هفت درصدی حملات علیه نقاط پایانی پروتکل دسک‌تاپ راه دور[8] وجود دارد که معمولاً دستگاه‌هایی هستند که کارمندان برای دسترسی از راه دور به منابع سازمانی استفاده می‌کنند. این هشدار همچنین در مورد حملات فیشینگ با موضوع کووید-۱۹ توزیع بدافزار، ثبت دامنه‌های جدید مرتبط با کووید-۱۹، حملات علیه زیرساخت‌های دسترسی از راه دور و دورکاری هشدار می‌دهد.

۲- کرونا و افزایش جرائم سایبری

ویروس خطرناک اقدام به ایجاد تغییرات جدید همچون فرایند دورکاری کارمندان شد تا به این نحو کمی با کووید-۱۹ مقاومت کنند. با این وجود ویروس کرونا در این زمینه نیز تأثیرگذار بود و به شکلی غیرمستقیم آسیب‌هایی جدی به مشاغل اینترنتی وارد کرد. با افزایش میزان دورکاری به ویژه در مشاغل الکترونیکی اهمیت امنیت سایبری نیز افزایش یافت و اکنون این حوزه یکی از حیاتی‌ترین بخش‌های مشاغل مختلف به حساب می‌آید. نادیده‌گرفتن امنیت سایبری می‌تواند باعث استخراج غیرقانونی داده‌ها شود و عوارض مخربی را به جای بگذارد.

با وجود آن که سازمان‌های امنیتی تلاش داشته‌اند که امنیت سایبری را گسترش دهند اما تحقیقات

7- https: //www. us-cert. gov/ncas/alerts/aa20-099a, accessed on April 24, 2020
8- RDP

نشان داده که شیوع ویروس کرونا باعث رشد شگفت آور حملات سایبری و کلاهبرداری‌های اینترنتی شده است. به دنبال این مسائل تصمیم گرفته شد تا نگاهی بر روی تأثیرات کرونا بر امنیت سایبری انداخته شود و بررسی‌های لازم صورت بگیرد. محدودیت‌های اعمال شده از سوی دولت‌های مختلف برای مقابله با ویروس کرونا و جلوگیری از شیوع این بیماری باعث شده تا عموم کارمندان به صورت دورکار فعالیت کنند. به دنبال این مسئله فعالیت‌ها در حوزه کاری و زندگی شخصی افراد با کمک فناوری و از طریق اینترنت گسترش پیدا کرده است. با وجود آن که افزایش نیاز به فناوری‌های مختلف در این دوران بیشتر احساس می‌شود، برخی از مشاغل و شرکت‌ها همچنان از امنیت سایبری مناسبی برخوردار نیستند و برای کارمندان دورکار خود سیستم امنیتی درستی را طراحی نکرده‌اند.

در ژوئن ۲۰۲۰ شرکت سوئیس اینفو با استفاده از اطلاعات مرکز امنیت سایبری ملی گزارشی را تهیه کرد که نشان می‌داد سیصد و پنجاه حمله سایبری طی یک ماه در سوئیس رخ داده است. میزان حملات سایبری پیش از شیوع ویروس کرونا در این کشور تنها یکصد مورد در ماه بود. براساس این تحقیقات علت اصلی افزایش این حملات فعالیت خانگی کارمندان بوده است. به دنبال این مسائل سازمان اف بی‌آی طی تحقیقات خود اعلام کرد که هم‌اکنون روزانه بیش از چهار هزار حمله سایبری صورت می‌گیرد که خبر از رشد چهارصد درصدی حملات می‌دهد. گفتنی است؛ سازمان اینترپل نیز تمامی شرکت‌ها را از موج جدید حملات سایبری مطلع کرده و اعتقاد دارد این حملات به صورت روزانه افزایش پیدا می‌کنند.

در عین حال، شاهد تغییر جالبی در جرائم فیزیکی در ابتدای همه‌گیری هستیم. شیکاگو که به جنایات خشن خود معروف است، از زمان شیوع بیماری همه گیر، شاهد کاهش چهل و دو درصدی دستگیری‌های مواد مخدر بوده است. پس از قرنطینه کووید-۱۹ در شیکاگو ده درصد کاهش در تمام جرائم وجود داشته است و این روند در سطح جهانی مشاهده شده است. علاوه بر این، حتی مناطقی که بالاترین سطح خشونت را در خارج از مناطق جنگی دارند، قتل و سرقت کمتری را گزارش می‌کنند. در واقع، حتی آنتونیو گوترش، دبیرکل سازمان ملل متحد، نسبت به افزایش شدید این حوادث ابراز نگرانی کرد و از دولت‌ها خواست حمایت و منابع بیشتری را برای قربانیان فراهم کنند. این مثال‌های مختلف نشان می‌دهد که بسیاری از مجرمان و سندیکای‌های جنایی زمانی که روال عادی زندگی‌شان با شروع همه‌گیری مختل می‌شد، به دنبال ابزارهای جایگزین برای توهین بودند. ارزشمند است که این الگوها را از

منظر دانشگاهی بیشتر مورد بررسی قرار دهیم، زیرا می‌تواند روشن‌تر کند که چگونه سازمان‌ها و افراد می‌توانند بهتر از خود در برابر تهدیدات امنیت سایبری در حال افزایش محافظت کنند.

۳- مبانی نظری

وقتی صحبت از توصیف و تعریف جرائم سایبری و قربانی‌شدن فیشینگ می‌شود، نظریه فعالیت روزانه رایج است. این نظریه در ابتدا توسط کوهن و فلسون ارائه شد و اصل آن تلاقی فیزیکی بین یک مجرم باانگیزه، یک هدف مناسب و فقدان نگهبانی توانا است. این نظریه یکی از محبوب‌ترین نظریه‌ها در زمینه جرم‌شناسی است، زیرا قربانی را به‌عنوان یک شرکت‌کننده فعال در جرم می‌داند و اعمال او (یا عدم وجود آن) می‌تواند در وقوع یا عدم وقوع جرم تأثیر داشته باشد. همچنین استدلال می‌کند که احتمال وقوع جرم تحت تأثیر فعالیت‌های روزانه (از جمله کار، خانواده، اوقات فراغت، و فعالیت‌های مصرفی) است. گزاره اصلی نظریه این است که میزان بزه دیدگی مجرمانه زمانی افزایش می‌یابد که همگرایی در مکان و زمان سه عنصر حداقلی نقض غارتگرانه با تماس مستقیم وجود داشته باشد (Cohen and Felson, 1979,589). علاوه بر این، فعالیت‌های روزانه توسط کوهن و فلسون به‌عنوان «فعالیت‌های مکرر و رایجی که نیازهای اساسی جمعیت و فردی را تأمین می‌کند، کار رسمی و همچنین تهیه غذای استاندارد، سرپناه، خروجی‌های جنسی، اوقات فراغت، اجتماعی، تعامل، یادگیری و فرزندآوری» تعریف می‌شود.

فعالیت روزانه به طور گسترده در زمینه جرائم سایبری استفاده می‌شود. به‌عنوان مثال، لوکفلدت و یار در (۲۰۱۶) یک تحلیل نظری و تجربی در سطح فردی انجام دادند و دریافتند که عناصر خاصی مانند دیده‌شدن در رسانه‌های اجتماعی، بیشتر از سایرین کاربرد دارند. نتایج مشابهی نیز در سطح ملی یافت شد که در آن کشورهای ثروتمندتر هدف حملات فیشینگ هستند (Kigerl,2012). علاوه بر این، رینز در (۲۰۱۳) شواهدی را ارائه می‌دهد که نشان می‌دهد افرادی که از اینترنت برای بانکداری و یا ایمیل یا پیام‌های فوری استفاده می‌کنند، حدود پنجاه درصد بیشتر از دیگران قربانی سرقت هویت می‌شوند. به طور مشابه، رفتارهای خرید و دانلود آنلاین خطر قربانی‌شدن را تا حدود سی درصد افزایش داد. این مطالعات نشان می‌دهد که تئوری فعالیت‌های روزانه می‌تواند جرائم فیزیکی و سایبری را با موفقیت توضیح دهد. درحالی‌که سایر نظریه‌های جرم‌شناسی مانند بازدارندگی، انتخاب عقلانی و یادگیری اجتماعی وجود دارد فعالیت‌های روزانه بیشترین استفاده را در زمینه جرائم سایبری داشته است. فرضیه مطالعه حاضر این است که کسانی که قبل از شروع همه‌گیری مرتکب جرم شده‌اند دست از کار نکشیده‌اند، بلکه روش‌های خود

را برای سازگاری با شرایط عادی جدید تغییر داده و از جرم فیزیکی به جرم خیابانی تغییر داده‌اند.

به دلیل قرنطینه اولیه جهانی کووید-۱۹ اکثریت افراد نمی‌توانستند بیرون بروند و نیازهای خود را شخصاً برآورده کنند چه به دلیل بسته‌بودن فروشگاه‌ها و چه به دلیل ایمن‌نبودن در اماکن عمومی. بنابراین، بیشتر مردم عادت‌های خود را تغییر دادند و از حضور فیزیکی به فعالیت‌های روزانه آنلاین روی آوردند. بسیاری در حال حاضر هنوز کار می‌کنند، مطالعه می‌کنند، ورزش می‌کنند و محصولات را در امنیت خانه‌های خود مصرف می‌کنند. براساس تئوری فعالیت‌های روزانه، این تغییر در عادات و سبک زندگی همچنین باعث تغییر در محیطی می‌شود که جرم در آن رخ می‌دهد. از آن جایی که اکثر مردم در خانه مانده‌اند، سرقت، قتل و تجاوز کاهش یافته است. با این حال، انواع دیگر جرائم مانند سرقت وسیله نقلیه، خشونت خانگی و سرقت از مشاغل تجاری خالی مانده، جرائم ناشی از نفرت و کلاهبرداری‌های مالی افزایش یافته است. در حال حاضر شواهدی از تأثیر کووید-۱۹ بر جرم وجود دارد و ما قطعاً شاهد تغییر در شیوه‌های مجرمان هستیم زیرا آن‌ها نیز با واقعیت جدید فاصله‌گذاری اجتماعی سازگار می‌شوند.

۴- روش شناسی

با توجه به ماهیت منحصر به فرد وضعیت کووید-۱۹ ما هنوز در مرحله جمع‌آوری داده‌ها و درک پیامدهای کامل این همه‌گیری هستیم. تقریباً بر هر جنبه‌ای از زندگی ما تأثیر گذاشته است، از جمله نحوه ارتکاب جرم. برای اهداف مطالعه حاضر، نویسنده تعدادی از منابع عمومی در دسترس مانند مقالات خبری، گزارش‌های دولتی و نشریات بخش خصوصی را بررسی می‌کند. برای نشان‌دادن این که چگونه کووید-۱۹ بر جنایت تأثیر گذاشته است، مطالعه ما به بولتن کارگروه ویژه کلاهبرداری سایبری سرویس مخفی ایالات متحده آمریکا[9] که در آوریل ۲۰۲۰ منتشر شد، ارجاع می‌دهد. هدف این نشریه شناسایی روندها و منابع فعلی و ارائه راهنمایی برای افراد و سازمان‌ها برای جلوگیری از قربانی‌شدن است که این یک ارتباط رسمی از طرف دولت ایالات متحده است آمریکا و براساس داده‌های قابل اعتماد و جامعی است که آژانس به آن‌ها دسترسی دارد. منبع دیگر برای این مطالعه داده‌ها و بیانیه‌های مطبوعاتی اداره تحقیقات فدرال[10] است. این منابع برای تجزیه و تحلیل روندها و الگوهای رفتار مجرمانه در زمان شروع همه‌گیری استفاده می‌شود.

9- USSS
10- FBI

۵- نتایج

۵-۱- کلاهبرداری‌های محرک

در سال ۲۰۲۰، کنگره ایالات متحده آمریکا یک بسته بزرگ کمکی و محرک کووید-۱۹ را تصویب کرد. بولتن کارگروه کلاهبرداری سایبری نشان داد که این آژانس شاهد افزایش کلاهبرداری در بخش محرک است و انتظار دارد این روند در سراسر همه‌گیری ادامه یابد. برخی از تکنیک‌هایی که کلاهبرداران استفاده می‌کنند، جعل مقامات خزانه‌داری ایالات متحده آمریکا و درخواست از افراد برای ارائه اطلاعات شناسایی شخصی[11] برای دریافت سهم خود از محرک است. علاوه بر ایمیل، متخلفان همچنین از پیامک، تماس‌های خودکار و دیگر پلتفرم‌های پیام‌رسانی برای تماس با قربانیان احتمالی استفاده می‌کنند. بازیگران مجرم از لینک‌هایی در متون استفاده می‌کنند تاگیرندگان را به وب‌سایت‌هایی هدایت کنند تا بتوانند اطلاعات شخصی و مالی و همچنین ایمیل‌ها و رمز عبور خود را وارد کنند. نکته جالبی که USSS در گزارش خود به آن اشاره می‌کند این است که شرکای خارجی آن‌ها نیز شروع به مشاهده پیام‌های مشابه کرده‌اند. بنابراین، اگرچه ممکن است خود جنایت جدید نباشد، زمینه و به موقع‌بودن کلاهبرداری‌های فیشینگ آن‌ها را مرتبط می‌سازد و احتمال کلیک‌کردن روی پیوندها را افزایش می‌دهد.

۵-۲- ایمیل‌های کووید-۱۹ با پیوست‌های مخرب

یکی دیگر از سناریوهای فیشینگ مورد استفاده در زمینه همه‌گیری، استفاده از ایمیل‌های قانونی سازمان‌های مختلف در رابطه با به‌روزرسانی‌های کووید-۱۹ است. همان‌طور که این ارتباط بیشتر می‌شود، مهاجمان شروع به استفاده از این آشنایی می‌کنند. برای مثال، مجرمان پیوست‌های مخربی را جاسازی می‌کنند که هم افراد و هم شرکت‌ها را هدف قرار می‌دهد. هدف آن‌ها نصب بدافزار از راه دور برای جمع‌آوری اعتبار، نصب کی لاگرها یا قفل‌کردن سیستم‌های باج افزار است. USSS تأکید می‌کند که تأثیر این حملات ممکن است فوری نباشد، اما ممکن است در آینده منجر به به خطر انداختن ایمیل‌های تجاری یا سایر کلاهبرداری‌ها شود. پیامد این یافته برای شرکت‌ها این است که آن‌ها باید محتاط‌تر باشند زیرا مهاجمان می‌توانند به طور بالقوه به‌عنوان فروشندگان، اعضای زنجیره تأمین یا سایر نهادهای آشنا

11- PII

ظاهر شوند که در صورت جعل ممکن است آگاهی را افزایش ندهند.

سناریوی دیگر برای ایمیل‌های فیشینگ در طول همه‌گیری مربوط به افرادی است که ایمیل‌هایی را دریافت می‌کنند که در ظاهر از یک بیمارستان ارسال می‌شوند و به آن‌ها اطلاع می‌دهند که ممکن است با فردی که تست کووید-۱۹ مثبت شده در تماس بوده باشند. ایمیل به‌گیرنده دستور می‌دهد که فایلی را دانلود کند، آن را پر کند و برای آزمایش بیشتر به نزدیک‌ترین بیمارستان بیاورد. در این جا نیز مهاجمان کدهای مخرب را در فایل جاسازی کرده‌اند و هدف آن‌ها سرقت اطلاعات ورود به سیستم، جست‌وجوی کیف پول‌های ارزهای دیجیتال، کشف اشتراک‌های باز در شبکه و دریافت آدرس‌ای پی است. یکی دیگر از انواع این کلاهبرداری، تغییر نام وزارت بهداشت و خدمات انسانی ایالات متحده آمریکا است. این ایمیل‌ها تأمین‌کنندگان احتمالی تجهیزات پزشکی را هدف قرار می‌دهند و از آن‌ها درخواست می‌کنند تا هرگونه تجهیزات پزشکی را ارائه دهند.

۳-۵- تحقیقات کووید-۱۹

به گفته اداره تحقیقات فدرال، موارد جرائم سایبری از زمان همه‌گیری سیصد درصد افزایش یافته است. مرکز شکایات جرائم اینترنتی این اداره[۱۲] اعلام کرد که اکنون روزانه بین سه هزار تا چهار هزار شکایت امنیت سایبری دریافت می‌کند که از میانگین یک هزار شکایت در روز بیشتر از قبل شیوع کووید-۱۹ است. علاوه بر این، اداره تحقیقات فدرال ادعا می‌کند که این به این دلیل است که اکثر فعالیت‌های روزانه ما اکنون به صورت آنلاین انجام می‌شود و کارگران تازه کار از راه دور حتی در مورد اقدامات امنیتی اولیه دانش محدودی دارند. علاوه بر این، آژانس بسیاری از حملات را به دولت-ملت‌هایی نسبت می‌دهد که به دنبال آخرین یافته‌های تحقیقات کووید-۱۹ هستند.

۶- بحث

کووید-۱۹ هنوز یک وضعیت در حال توسعه با ناشناخته‌های بسیاری است. همان‌طور که ما به طور خستگی‌ناپذیر تحقیقات پزشکی را در مورد کروناویروس جدید انجام می‌دهیم و بر بهبود اقتصاد جهانی تمرکز می‌کنیم، باید به تغییرات در جامعه نیز توجه کنیم. هیچ‌کس قبلاً چنین چیزی را تجربه نکرده است و درحالی‌که ما هنوز در مرحله جمع‌آوری داده‌ها هستیم، مهم است که بتوانیم برخی از نتایج را بگیریم و

12- IC3

الگوهایی را شناسایی کنیم که می‌توانند به پیشرفت جامعه ما کمک کنند. هدف کار ما پاسخ به این سؤال بود که پیامدهای کووید-۱۹ بر جرم در شروع همه‌گیری چیست؟ براساس داده‌های ثانویه‌ای که نویسنده بررسی کرد، این مطالعه تغییراتی را در رفتار مجرمانه و نحوه برخورد مجرمان به جرم در مراحل اولیه اپیدمی جهانی شناسایی کرد.

یافته‌های ما نشان می‌دهد که در ابتدا انواع خاصی از جرائم فیزیکی مانند سرقت، تجاوز و قتل کاهش یافت، اما موارد دیگر مانند خشونت خانگی، سرقت خودرو و کلاهبرداری‌های آنلاین در حال افزایش بودند. از طریق داده‌های ثانویه، نویسنده توانست برای این فرضیه که ما شاهد تغییر جنایت در مراحل اولیه همه‌گیری هستیم، پشتیبانی پیدا کند. بسیاری از محققین موافق هستند که مجرمان فرصت طلب هستند و رویدادهای بزرگ را فرصت می‌بینند (Watson,2005)و(Okoye & Gbegi,2013). وضعیت کووید-۱۹ نیز متفاوت نیست. در واقع، این یک فرصت عالی برای مجرمان مبتکر است زیرا آن‌ها از یکی از اساسی‌ترین شرایط انسانی (ترس) استفاده می‌کنند (McManus,2011)و(Smith,2009). ثابت شده است که ترس بر ادراکات سوگیری می‌کند و بر تصمیم‌گیری تأثیر می‌گذارد (Petty & Briñol,2015). بنابراین، در یک بیماری همه گیر که در آن مردم نگران زندگی خانواده و عزیزان خود هستند، آسیب پذیرتر می‌شوند و در نتیجه بیشتر در معرض فیشینگ و سایر اشکال مهندسی اجتماعی قرار می‌گیرند.

کووید-۱۹ پیامدهای مهمی بر جامعه دارد. وقتی صحبت از جرم و جنایت به میان می‌آید، شاهد تعداد فزاینده‌ای از کلاهبرداری‌ها هستیم و بسیاری از آن‌ها با دقت طراحی شده‌اند تا وضعیت فعلی را منعکس کنند. از آن جایی که بیشتر افراد در خانه کار می‌کنند، احتمالاً از شبکه‌های خانگی محافظت نشده با ویژگی‌های امنیتی محدود استفاده می‌کنند. زوم، محبوب‌ترین پلتفرم برای کنفرانس ویدیویی در حال حاضر، دارای چندین مشکل امنیتی و حریم خصوصی است. این فقدان نگهبانی توانا و آسیب‌پذیری قربانیان، آن‌ها را به اهداف مناسبی برای مجرمان باانگیزه تبدیل می‌کند که اکنون از حوزه فیزیکی به حوزه سایبری می‌روند. از آن جایی که وقایع هنوز در حال آشکارشدن هستند، انتظار داریم در آینده نزدیک شاهد وقوع جرائم سایبری بیشتری درحالی‌که دستورات اقامت در خانه وجود دارد، باشیم.

۷- محدودیت‌ها و کار آینده

کرونا چالش‌های منحصر به فردی را برای همه جنبه‌های زندگی ما ارائه می‌دهد. این وضعیت هنوز ادامه دارد و باید داده‌های بیشتری جمع‌آوری شود تا درک بهتری از تأثیر کامل همه‌گیری بر جامعه داشته

باشیم. این مقاله مطالعه‌ای اکتشافی در مورد موضوعی بسیار گسترده است که ما هنوز در مورد آن اطلاعات کمی داریم. بنابراین، همکاران ما تشویق می‌شوند که به تحقیق در مورد پیامدهای کووید-۱۹ بر جرائم سایبری ادامه دهند. هرچه اطلاعات بیشتری در مورد این موضوع پیچیده جمع‌آوری کنیم، محافظت از افراد و شرکت‌ها و آموزش آن‌ها در مورد اقداماتی که می‌توانند برای جلوگیری از قربانی‌شدن حملات فیشینگ انجام دهند، آسان‌تر خواهد بود. نویسنده چالش جمع‌آوری داده‌های اولیه در زمان‌های نامشخص را تصدیق می‌کند. استفاده از مثلث‌سازی یک تکنیک ارزشمند برای بهبود درک ما از این مشکل پیچیده و افزودن دقت بیشتری به مطالعات آینده است (Jones & Bugge,2006).

۸- مفاهیم برای تئوری و عمل

مطالعه حاضر به ایجاد مجموعه‌ای از دانش از کار علمی در مورد کروناویروس جدید کمک می‌کند. در این زمان‌های بی‌سابقه، برای محققان مهم است که به جنبه‌های مختلف چگونگی تأثیر کووید-۱۹ بر جامعه بپردازند. نویسنده به طور خاص به بررسی جرم و جنایت و چگونگی تغییر آن از فضای فیزیکی به فضای مجازی با توجه به محیط و شرایط جدید می‌پردازد. مجرمان باهوش و فرصت طلب هستند، بنابراین همیشه به دنبال راه‌های جدیدی برای بهره‌برداری از ضعف‌های انسانی هستند. همه‌گیری فرقی نمی‌کند و از طریق کار فعلی، نویسنده قصد دارد به الگوها و روندهایی اشاره کند که محققان و پزشکان می‌توانند در آینده از آن‌ها استفاده کنند.

مطالعه ما می‌تواند به محققین کمک کند تا ایده نظریه فعالیت روزانه را در زمینه تغییر الگوهای جرم و جنایت ایجاد کنند. این یافته‌ها با کار قبلی در زمینه بسط این نظریه برای توضیح جرائم سایبری سازگار است (Yar,2005)و(Jansen & Leukfeldt,2016)و(Holt & Bossler,2008). در واقع، نویسنده به هر سه جنبه آن اشاره می‌کند. اهداف مناسبی که اکنون در خانه قرنطینه شده‌اند، فقدان نگهبانی توانمند به‌عنوان کارکردهای IT و امنیتی سازمانی کنترل بسیار کمی بر محیط خانه و سیستم‌های کارمندان دارند و افراد با انگیزه. مجرمانی که اکنون از وضعیت کووید-۱۹ برای ایجاد کلاهبرداری‌های فیشینگ مرتبط و معتبرتر و حمله به مراکزی که در حال تحقیق و توسعه بر روی واکسن‌های جدید هستند سوءاستفاده می‌کنند.

از نظر پیامدهای عملی، این مطالعه به سازمان‌ها توصیه می‌کند که از این زمان برای آموزش مشتریان و کارکنان خود در مورد بهترین شیوه‌های کار در خانه استفاده کنند. از نکات ساده‌ای مانند نحوه ایمن‌سازی جلسات تا کارگاه‌های آموزشی فیشینگ با هدف افزایش آگاهی در مورد کلاهبرداری‌های

احتمالی موجود در آن جا. اگرچه وضعیت کنونی بی‌سابقه است و میلیون‌ها نفر باید به سرعت راه‌هایی برای کار در خانه پیدا می‌کردند، اما اکنون که اوضاع در حال حل‌شدن است و ما باید تمرکز خود را به ارائه نگهبانی توانا و تأمین دارایی‌های خود تغییر دهیم. به‌عنوان مثال، ما می‌توانیم منابع اضافی مانند شبکه‌های خصوصی مجازی[۱۳] فراهم کنیم تا کلاینت‌ها بتوانند یک کانال رمزگذاری شده برای برقراری ارتباط با سرورها و احراز هویت چند عاملی[۱۴] برای بهبود کنترل‌های دسترسی داشته باشند. علاوه بر این، این زمان بسیار خوبی برای انجام تعمیر و نگهداری و ارتقاء شبکه‌های شرکتی است، زیرا باعث ایجاد حداقل وقفه برای کاربران می‌شود.

نتیجه

کووید-۱۹ تقریباً همه جنبه‌های زندگی ما را تحت تأثیر قرار داده است و درحالی‌که ما هنوز در حال تطبیق با انجام انواع فعالیت‌های آنلاین هستیم، باید بدانیم که می‌توانیم حتی به راحتی در خانه‌هایمان قربانی شویم. ما نباید نگهداری از خود را پایین بیاوریم و اجازه دهیم ترس بر ما مسلط شود. برعکس، ما باید بیش از هر زمان دیگری هوشیار باشیم زیرا جنایتکاران همیشه به دنبال راه‌های جدیدی برای حمله به ما هستند. یافته‌های پژوهش نشان می‌دهد که درحالی‌که برخی از جرائم در ابتدای همه‌گیری کاهش یافته است، جرائم سایبری در حال افزایش است، زیرا نیازی به تماس فیزیکی بین قربانی و مجرم نیست. سازمان‌ها و افراد باید هرگونه ارتباطی را که دریافت می‌کنند به دقت ارزیابی کنند و همیشه منبع را تأیید کنند. ما می‌توانیم از تئوری فعالیت‌های روزانه برای جست‌وجوی راه‌های نوآورانه برای محافظت از خود و دارایی‌های مان استفاده کنیم. درست مانند جنایتکاران، ما باید تمرکز خود را تغییر دهیم و بررسی کنیم که چگونه می‌توانیم در خانه امن‌تر بمانیم، هم از نظر فیزیکی و هم از نظر مجازی.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

13- VPN
14- MFA

منابع

- Birk, D. , Gajek, S. , Grobert, F. , & Sadeghi, A. -R. 2007, Phishing phishers-observing and tracing organized cybercrime. Second International Conference on Internet Monitoring and Protection (ICIMP 2007), 1-5 July 2007, San Jose, CA, USA.
- Cohen, L. E. , & Felson, M. 1979, Social change and crime rate trends: A routine activity approach. American sociological review.
- Grabosky, P. 2015, Organized cybercrime and national security. In Cybercrime Risks and Responses.
- Groff, E. R. 2007, Simulation for theory testing and experimentation: An example using routine activity theory and street robbery. Journal of Quantitative Criminology.
- Holt, T. J. , & Bossler, A. M. 2008, Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1).
- Jansen, J. , & Leukfeldt, R. 2016, Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1).
- Jennings, W. G. , Higgins, G. E. , Tewksbury, R. , Gover, A. R. , & Piquero, A. R. 2010, A longitudinal assessment of the victim-offender overlap. Journal of Interpersonal Violence, 25(12).
- Jian, J. , Chen, S. , Luo, X. , Lee, T. , & Yu, X. 2020, Organized Cyber-Racketeering: Exploring the Role of Internet Technology in Organized Cybercrime Syndicates Using a Grounded Theory Approach. IEEE Transactions on Engineering Management.
- Jones, A. , & Bugge, C. 2006, Improving understanding and rigour through triangulation: an exemplar based on patient participation in interaction. Journal of advanced nursing, 55(5).
- Kigerl, A. 2012, Routine activity theory and the determinants of high cybercrime countries. Social science computer review, 30(4).
- Kirda, E. , & Kruegel, C. 2006, Protecting users against phishing attacks. The Computer Journal, 49(5).
- Laszka, A. , Johnson, B. , Schöttle, P. , Grossklags, J. , & Böhme, R. 2013 و Managing the Weakest Link. In ComputerSecurity-ESORICS.
- Leukfeldt, E. R. , & Yar, M. 2016, Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3).
- Lusthaus, J. 2013, How organised is organised cybercrime? Global Crime, 14(1).
- Marcum, C. D. , Higgins, G. E. , Freiburger, T. L. , & Ricketts, M. L. 2014, Exploration of the cyberbullying victim/offender overlap by sex. American Journal of Criminal Justice, 39(3).
- McManus, S. 2011, Hope, fear, and the politics of affective agency. Theory & Event, 14(4).
- Okoye, E. I. , & Gbegi, D. 2013, Forensic accounting: A tool for fraud detection and prevention in the public sector.
- Reyns, B. W. 2013, Online routines and identity theft victimization: Further expanding

routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2).
- Reyns, B. W. 2015, A routine activity perspective on online victimisation. Journal of Financial Crime, 22(4).
- Robinson, M. B. 1999, Lifestyles, routine activities, and residential burglary victimization. Journal of Crime and Justice, 22(1).
- Shelley, L. I. 2003, Organized crime, terrorism and cybercrime. Security sector reform: Institutions, society and good governance.
- Smith, R. 2009, Understanding entrepreneurial behaviour in organized criminals. Journal of Enterprising Communities: People and Places in the Global Economy.
- Sood, A. K. , & Enbody, R. J. 2013, Crime-ware-as-a-service a survey of commoditized crimeware in the underground market. International journal of critical infrastructure protection, 6(1).
- Tewksbury, R. , & Mustaine, E. E. 2003, College students' lifestyles and self-protective behaviors: Further considerations of the guardianship concept in routine activity theory. Criminal Justice and Behavior, 30(3).
- Van Wegberg, R. , Tajalizadehkhoob, S. , Soska, K. , Akyazi, U. , Ganan, C. H. , Klievink, B. , Christin, N. , & Van Eeten, M. 2018, Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. 27th USENIX Security Symposium.
- Watson, M. 2005, Environmental crime in the United Kingdom. Eur. Envtl. L. Rev. , 14.
- Wehinger, F. 2011, The Dark Net: Self-regulation dynamics of illegal online markets for identities and related services. European Intelligence and Security Informatics Conference, September 12-14, 2011, Athens, Greece.
- Yar, M. 2005, The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4).
- Yip, M. , Shadbolt, N. , Terrapins, T. , & Webber, C. 2012, The digital underground economy: A social network approach to understanding cybercrime.

Legal Civilization

ISSN: 2783-1841
ISSN: 2873-1922

No.12-Autumn 2022