

## بسمه تعالی

از: محمد صالح سوزنچی

به: رئیس پلیس فتا همدان

موضوع: اعلام و معرفی منبع اصلی انتشار نامه ارسالی، از نیروی انتظامی جمهوری اسلامی ایران، به دادستان محترم کل کشور- حجت الاسلام والمسلمین حاج آقا منتظری، با موضوع دسترسی به افزونه فیلترینگ، به تاریخ ۱۳۹۶/۰۹/۲۹ و شماره ۱۴/۱۱۷/۶/۱۲/۶/۱۲۵، که توسط ضابطین محترم پلیس فتا در تفتیش و بازرسی از کیس کامپیوتر تحت بازداشت اینجانب کشف شده بود، بدین شرح می باشد:

با عرض سلام؛

احتراما همانگونه که مستحضرید، اینجانب محمد صالح سوزنچی، خوانده در پرونده کلاسه ۱۴۰۲۲۸۹۲۰۰۰۲۲۱۶۵۰۴ با شماره بایگانی ۰۲۰۱۶۴۱، در بازجویی سوم خود که در تاریخ ۹ اسفند ۱۴۰۲ و پیرامون موضوع همین پرونده صورت گرفته بود، در برگه اظهارات مطلع که آنرا امضا و اثر انگشت زده‌ام، متعهد شده بودم که تا تاریخ یکشنبه ۱۳ اسفند ۱۴۰۲ منبع اصلی انتشار نامه زیر را کشف و علت و نحوه دانلود شدن آنرا توضیح داده و در نهایت نتیجه را به سرهنگ زارعی، رئیس محترم پلیس فتا همدان گزارش بکنم.

طبقه بندی:			
شماره:	۱۴/۱۱۷/۶/۱۲/۶/۱۲۵		
تاریخ:	۱۳۹۶/۰۹/۲۹		
پیوست:	ندارد		

**فرماندهی**

از: نیروی انتظامی جمهوری اسلامی ایران  
به: دادستان محترم کل کشور- حجت الاسلام والمسلمین حاج آقا منتظری  
موضوع: دسترسی به افزونه فیلترینگ

سلام علیکم

**با صلوات بر محمد(ص) و آل محمد(ص) و عرض احترام به استحضار می رساند:**

مهم ترین راهکار برای ایجاد محدودیت در فضای مجازی، بهره گیری از فیلترینگ است که امروزه در اغلب کشورها بر پایه خط مشی های گوناگون و با درجاتی از شدت و ضعف رایج می باشد. در این راستا پلیس اطلاعات و امنیت عمومی مسئولیت اشراف بر حوزه های "ضد امنیتی، ساماندهی کسب و کارهای اینترنتی و موضوع های علیه عفت و اخلاق عمومی در فضای مجازی" را بر عهده دارد که پیشگامانه را برعهده دارد که برای تحقق اهداف سازمانی، بهره گیری از ظرفیت فیلترینگ و مسدودسازی به عنوان خاکیز بنیادی و یکی از شاخص های اثرگذار برای پاک سازی و ایجاد امنیت در فضای مجازی، اجتناب ناپذیر می باشد؛ از این رو با عنایت به هماهنگی انجام شده، به منظور تطابق مأموریت های تخصصی در این حوزه با محورهای متعدد تعریف شده درافزونه کارگروه تعیین مصادیق مجرمانه؛ خواهشمند است دستور فرمایید امکان دسترسی مستقیم پلیس اطلاعات و امنیت عمومی به افزونه فیلترینگ در شش حوزه تخصصی زیر با قابلیت گزارش گیری مستقل ومجزا(سلسله مراتبی) را فراهم نموده و نتیجه را به این نیرو اعلام نمایند.

الف) محتوای علیه عفت و اخلاق عمومی  
ب) محتوای علیه مقدسات اسلامی  
ج) محتوای علیه امنیت و آسایش عمومی  
د) محتوای علیه مقامات و نهادهای دولتی و عمومی  
ح) محتوای مجرمانه مرتبط با انتخابات مجلس شورای اسلامی  
ط) محتوای مجرمانه مرتبط با انتخابات ریاست جمهوری

فرمانده نیروی انتظامی جمهوری اسلامی ایران

سرتیپ پاسدار حسین اشتری

رئیس محترم پلیس فتا همدان، جناب سرهنگ زارعی همانطور که در مستندات بعدی بخوبی مشهود است، منبع اصلی نشت و انتشار نامه فوق‌الذکر که ظاهراً مورد توجه خاص سردار مجید [احتمالاً] نیز قرار گرفته است، بطوریکه ایشان در راستای پیگیری این موضوع، دوتن از متخصصان فتای تهران را ماموریت کرده بودند که به همدان آمده و در بازجویی از بنده متوجه بشوند که این نامه چرا و چگونه بدست اینجانب رسیده است.

**Subject:** دسترسی به افزونه فیلترینگ  
**From:** <pava@internet.ir> پلیس امنیت  
**Date:** 2/8/2018, 9:52 AM  
**To:** <nezarat@internet.ir> اداره نظارت  
**CC:** <pava@internet.ir> پلیس امنیت

با سلام  
با عنایت به هماهنگی‌های صورت گرفته با جناب آقای امیری تصویر مکاتبه درخواستی در خصوص دسترسی به افزونه فیلترینگ برای پاوا، ارسال می‌گردد  
با تشکر

— Attachments: —

IMG\_20180207\_0003.rar

401 kB

شوربختانه مشخص شد که منبع اصلی این نامه نیز مثل اکثر نامه‌ها و دیتاهای حاکمیتی و دولتی که به بر روی سیستم من به فراوانی یافت می‌شود، همگی رسماً یک منبع مشترک دارند. یعنی منبع اصلی آنها همان بکاپ ایمیل‌های ایمیل سرور هک شده دادستانی کل کشور (INTERNET.IR) است که در تاریخ ۱۳ آبان ۱۴۰۱ توسط هکرهای ناشناس هک شدند و بکاپ‌هایش را بصورت عمومی در فضای مجازی منتشر ساختند.

**Mahdi Amiri**  
تا زمانی که گزارش خلاف واقع کارمندان دولت از تخلف اداری به جرم تبدیل نشود، مشکلات کشور...  
انتشار خبر و محتوای خلاف واقع که موجب تشویش آذهنان عمومی بشود جرم است و قرقی هم نمی‌کند که از سوی کارکنان اداری باشد یا نظامی یا اشخاص عادی  
۸ خرداد ۱۴۰۲ - ۲۱:۴۸

**Anonymous Opiran @anonopiran** · ۱۴۰۱/۸/۱۳، ۰۵:۱۸  
سرور ایمیل درگاه خدمات الکترونیک مصادیق محتوای مجرمانه زیر نظر دادستان کل کشور هک، و صدها سند و پیام مرتبط با فیلترینگ و محدود سازی اینترنت در ایران استخراج شد. ما این اطلاعات را در اختیار شما قرار می‌دهیم  
برای دانلود: <https://t.me/anonopiran>  
We Are Anonymous  
!Expect Us  
#Opiran

**Mahdi Amiri**  
بحث بر سر ناظر و ضامن نیست. در حال حاضر این تکذیبیه، گزارش خلاف واقع حساب میشود. یعنی...  
گرامی  
از شما که زمانی در کسوت ضابط دادگستری بودید تعجب می‌کنم که اینطور بی دقت هر حرف کذبی را مطرح می‌کنید.  
هیچ وقت سایت یا شبکه دادستانی در طول تاریخ هک نشد.  
آنچه مورد تهاجم قرار گرفت سرویس ایمیلی بود که راه اندازی، پشتیبانی و تامین امنیتش هم برعهده سازمان دیگری بود.  
و هیچ وقت هم تکذیب نشد.  
اتفاقاً آنچه اهمیت دارد، به هیچ وجه جنبه رسانه ای حوادث نیست.  
بلکه ریشه یابی امنیت است.  
مسئله نیروی انسانی متخصص امنیت است که روز به روز کمیاب تر می‌شود.  
مسئله هزینه ای است که مجلس و دولت باید برای تامین امنیت بپردازد و هیچ وقت تامین نمی‌شود.  
ما بقی فقط شوی رسانه ای است که هیچ حاصلی هم ندارد.  
ویرایش شده ۸ خرداد ۱۴۰۲ - ۲۱:۴۰

**Mahdi Amiri**  
ایمان  
پیام صوتی  
سایت internet.ir هیچ وقت و در هیچ زمانی هک نشده بلکه برای بازطراحی آن با رعایت تمهیدات امنیتی بیشتر برنامه ریزی شده است.  
امکان تعامل با کمیته فیلترینگ هم از طریق تمامی شبکه های اجتماعی داخلی (@netreport) و ایمیل (filter@internet.ir) فراهم بوده و هست.  
۲۱ اسفند ۱۴۰۱ - ۲۱:۵۶

مساله این است:  
**آیا در طول تاریخ وبسایت یا شبکه دادستانی کل کشور هک شده یا نشده است؟!**

مهندس امیری-معاون مدیرکل نظارت و پیگیری امور فضای مجازی دادستانی کل کشور  
و بازپرس ویژه رسیدگی به پرونده‌های قمارخانه‌های اینترنتی

اینجانب نیز همانند سایر افراد دیگر با اطلاع از این موضوع آنها را دانلود کردم و پس از بررسی مختصری متوجه یکسری مسائل مهمی شدم، که هریک در آینده نزدیک پتانسیل تبدیل شدن به یک تهدید ملی را داشتند. براین اساس بر خودم لازم دیدم که بر روی آنها کمی تحقیق کنم. برای همین منظور با مطالعه هر یک از این ایمیل‌ها، آندسته از محتواهایی که بنظر مهم می‌رسیدند را استخراج کرده و دستبندی می‌کردم تا بتوانم از هر یک از آنها و بسته به نوع نیازهایم مثل ارسال گزارش به نهادهای امنیتی از آنها استفاده نمایم.

دسترسی به افزونه فیلترینگ

**Subject:** دسترسی به افزونه فیلترینگ  
**From:** <pava@internet.ir> پلیس امنیت  
**Date:** 2/8/2018, 9:52 AM  
**To:** <nezarat@internet.ir> اداره نظارت  
**CC:** <pava@internet.ir> پلیس امنیت  
**X-Mozilla-Status:** 0001  
**X-Mozilla-Status2:** 10000000  
**Return-Path:** pava@internet.ir  
**Received:** from internet.ir (LHLO internet.ir) (94.232.175.83) by internet.ir with LMTP; Thu, 8 Feb 2018 09:53:10 +0330 (IRST)  
**Received:** from localhost (localhost [127.0.0.1]) by internet.ir (Postfix) with ESMTP id 55B45209C74; Thu, 8 Feb 2018 09:53:10 +0330 (IRST)  
**X-Spam-Flag:** NO  
**X-Spam-Score:** 1.061  
**X-Spam-Level:** \*  
**X-Spam-Status:** No, score=1.061 tagged\_above=-10 required=6.6 tests=[ALL\_TRUSTED=-1, BAYES\_00=-1.9, DNS\_FROM\_AHBL\_RHSBL=2.699, RCVD\_IN\_BRBL\_LASTTEXT=1.449, RDNS\_NONE=0.793, RP\_MATCHES\_RCVD=-1, T\_HELO\_NO\_DOMAIN=0.01, T\_KHOP\_THREADED=-0.01, T\_LONG\_HEADER\_LINE\_80=0.01, T\_NOT\_A\_PERSON=-0.01, T\_PUBLISHED\_DNSBLS\_BRBL=0.01, T\_THREAD\_INDEX\_BAD=0.01] autolearn=no  
**Received:** from internet.ir ([127.0.0.1]) by localhost (internet.ir [127.0.0.1]) (amavisd-new, port 10032) with ESMTP id MER\_zOB3ZFVZ; Thu, 8 Feb 2018 09:53:05 +0330 (IRST)  
**Received:** from localhost (localhost [127.0.0.1]) by internet.ir (Postfix) with ESMTP id 2D71C209C7E; Thu, 8 Feb 2018 09:53:05 +0330 (IRST)  
**X-Virus-Scanned:** amavisd-new at internet.ir  
**Received:** from internet.ir ([127.0.0.1]) by localhost (internet.ir [127.0.0.1]) (amavisd-new, port 10026) with ESMTP id V7viV6Dd4BrF; Thu, 8 Feb 2018 09:52:51 +0330 (IRST)  
**Received:** from internet.ir (internet.ir [94.232.175.83]) by internet.ir (Postfix) with ESMTP id 93077209C8B; Thu, 8 Feb 2018 09:52:51 +0330 (IRST)  
**Message-ID:** <1455997291.517335.1518070971062.JavaMail.root@internet.ir>  
**In-Reply-To:** <1518213591.517319.1518070820193.JavaMail.root@internet.ir>  
**MIME-Version:** 1.0  
**Content-Type:** multipart/mixed; boundary="-----\_Part\_517333\_410215790.1518070971044"  
**X-Originating-IP:** [92.61.185.5]  
**X-Mailer:** Zimbra 8.0.3\_GA\_5664 (ZimbraWebClient - FF49 (Win))/8.0.3\_GA\_5664  
**Thread-Topic:** دسترسی به افزونه فیلترینگ  
**Thread-Index:** yGBJUAmZmans1P3jzrwJLw1BTM+LpQ==

با سلام

با عنایت به هماهنگی‌های صورت گرفته یا جناب آقای امیری تصویر مکاتبه درخواستی در خصوص دسترسی به افزونه فیلترینگ برای پوا، ارسال می‌گردد  
با تشکر

Attachments:

IMG\_20180207\_0003.rar

401 kB

Search... CTRL + K

Local Folders افزونه فیلترینگ

افزونه فیلترینگ 5 Messages

Quick Filter

Reply Reply All Forward Archive Junk Delete

پلیس امنیت  
pava@internet.ir

To اداره نظارت <nezarat@internet.ir> 2/8/2018, 9:52 AM

Cc پلیس امنیت <pava@internet.ir>

دسترسی به افزونه فیلترینگ

با سلام  
با عنایت به هماهنگی های صورت گرفته با جناب آقای امیری تصویر مکاتبه درخواستی در خصوص دسترسی به افزونه فیلترینگ برای پاوا، ارسال می گردد  
با تشکر

1 attachment: IMG\_20180207\_0003.rar 401 kB

IMG\_20180207\_0003.rar 401 kB

Subject	Recipient	Correspondents	Date	Size
دسترسی به افزونه فیلترینگ	اداره نظارت	پلیس امنیت	2/8/2018, 9:52 AM	551 kB
دسترسی به افزونه فیلترینگ	اداره نظارت	پلیس امنیت	2/7/2018, 1:31 PM	550 kB
افزونه فیلترینگ	اداره نظارت	پلیس امنیت	1/16/2018, 7:34 AM	68.8 kB
Fwd: Re: Fwd: نیکو چت	سوه تعیین مصادیق	دبیر کارگروه تعیین مصادیق مجرمانه	8/23/2015, 11:57 AM	21.3 kB
asl19.org/fa/privacybadger - Privacy Badger	Saberi	اداره نظارت دبیرخانه کارگروه تعیین مصادیق	4/22/2015, 7:09 PM	5.4 kB

IMG\_20180207\_0003.rar

File Commands Tools Favorites Options Help

IMG\_20180207\_0003.rar - RAR 4.x archive, unpacked size 547,892 bytes

Name	Size	Type	Modified	CRC32
..		File folder		
IMG_20180207_0003.pdf	547,892	PDF Document	2/7/2018 12:42 PM	61061876

Selected 1 file, 547,892 bytes

Total 1 file, 547,892 bytes


Quick Launch (Ctrl+.)

File Home View Comment Protect Form Organize Convert Share Review Accessibility Bookmarks Help Format

IMG\_20180207\_0003

C:\Users\Saleh\AppData\Local\Temp\Rar\$Dla1876.36285\IMG\_20180207\_0003.pdf

طبقه بندی :  
 شماره : ۱۴/۱۱۷/۶/۱۲۴/۱۴۵  
 تاریخ : ۱۳۹۶/۰۹/۱۹  
 پیوست : ندارد



فرماندهی

از: نیروی انتظامی جمهوری اسلامی ایران  
 به: دادستان محترم کل کشور- حجت الاسلام والمسلمین حاج آقا منتظری  
 موضوع: دسترسی به افزونه فیلترینگ

سلام علیکم

با صلوات بر محمد(ص) و آل محمد (ص) و عرض احترام به استحضار می رساند:

مهم ترین راهکار برای ایجاد محدودیت در فضای مجازی، بهره گیری از فیلترینگ است که امروزه در اغلب کشورها بر پایه خط مشی های گوناگون و با درجاتی از شدت و ضعف رایج می باشد. در این راستا پلیس اطلاعات و امنیت عمومی مسئولیت اشراف بر حوزه های "ضد امنیتی، ساماندهی کسب و کارهای اینترنتی و موضوع های علیه عفت و اخلاق عمومی در فضای مجازی" با رویکرد پیشگیرانه را برعهده دارد که برای تحقق اهداف سازمانی، بهره گیری از ظرفیت فیلترینگ و مسدودسازی به عنوان خاکریز بنیادی و یکی از شاخص های اثرگذار برای پاک سازی و ایجاد امنیت در فضای مجازی، اجتناب ناپذیر می باشد؛ از این رو با عنایت به هماهنگی انجام شده، به منظور تطابق مأموریت های تخصصی در این حوزه با محورهای متعدد تعریف شده درافزونه کارگروه تعیین

Options... 1/1 97.06%

Search... CTRL + K

Local Folders افزونه فیلترینگ

افزونه فیلترینگ 5 Messages

Expression Search...

Subject	Recipient	Correspondent
دسترسی به افزونه فیلترینگ	اداره نظارت	پلیس امنیت
دسترسی به افزونه فیلترینگ	اداره نظارت	پلیس امنیت
افزونه فیلترینگ	اداره نظارت	پلیس امنیت
Fwd: Re: Fwd: نیکو چت	...تعیین مصادیق	ختوای مجرمانه
asl19.org/fa/privacybadger - Privacy Badger	Saberi	تعیین مصادیق

IMG\_20180207\_0003.rar

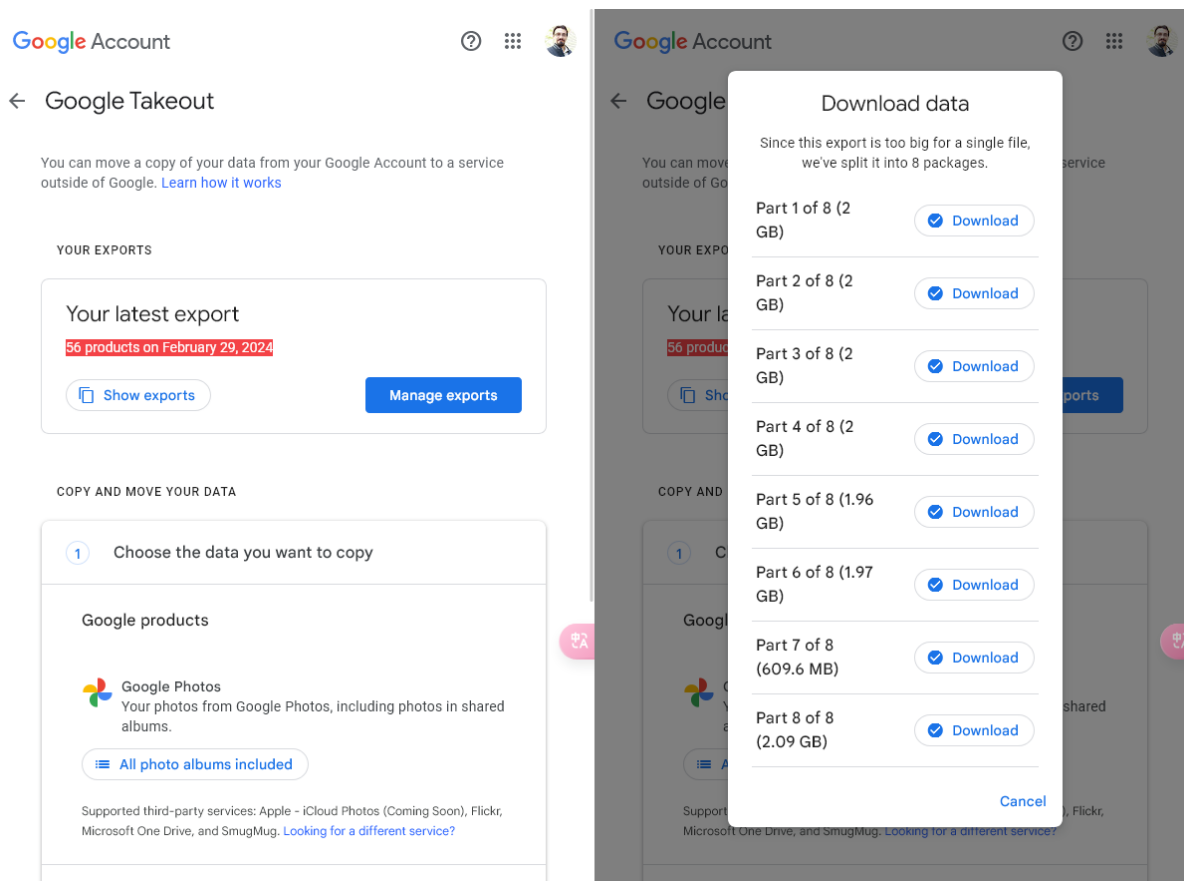
File Commands Tools Favorites Options Help

IMG\_20180207\_0003.rar - RAR 4.x archive, unpacked size 547,892 bytes

Name	Size	Type	Modified	CRC32
..		File folder		
IMG_20180207_0003.pdf	547,892	PDF Document	2/7/2018 12:42 PM	61061876

Selected 1 file, 547,892 bytes

در پایان نیز می‌بایست به این نکته اشاره کنم، با توجه به اینکه تا همین لحظه که فقط به ایمیل توانستم مجدداً دسترسی پیدا کنم. متوجه شدم که نمایندگان پلیس فتا تهران همراه خودشان ۶۰ گیگ از اطلاعات هارددیسک کامپیوترم و ۱۴٫۶ گیگ اطلاعات از ایمیل ([saleh.souzanchi@gmail.com](mailto:saleh.souzanchi@gmail.com)) اصلی بنده را برای سردار عزیز به تهران منتقل کرده‌اند تا ایشان بتوانند از نزدیک به همه اطلاعات اینجانب دسترسی و اشراف کامل داشته باشند.



بر این اساس بود که دیدم جهت محکم کاری بد نیست برای راهنمایی سردار عزیز، یک ویدیوی آموزشی مختصر هم تهیه کنم تا به ایشان نحوه آسان بررسی و صحت‌سنجی این مستندات را آموزش بدم. که انشالله به محض آنکه مجدد به گوشی دومم که در همان روز بازجویی بصورت موقت بازداشت شده بود، دسترسی پیدا کنم، آن را نیز در کانال زیر منتشر می‌سازم که دیگر جایی برای شک و شبهه باقی نمانده باشد:

<https://t.me/ToofanReports>

همچنین می‌بایست این موضوع را نیز به لطف ایت گزارش به اطلاع ایشان برسانم که با هزار سختی و مکافات که بخاطر عدم دسترسی به تجهیزاتم که اکنون نزد شما توقیف است ایجاد شده بود، بالاخره با موفقیت نسبی توانستم یکی از گزارش‌های تحقیقاتی‌ام را که ۱۰۰٪ مورد توجه ایشان قرار خواهد گرفت را به اتمام برسانم.

لذا تصمیم گرفتم بدینوسیله از سردار مجید و سایر همکاران محترم‌شان دعوت بعما بیاورم تا عضو کانال بنده بشوند تا بتوانند و از طریق در اسرع وقت در جریان انتشار کلیات و جزئیات این گزارش نیز قرار بگیرند. البته اگر این افتخار را به بنده حقیر متهم به کلاهبرداری بدهند.

محمد صالح سوزنچی



## کلاهبرداران چگونه و به چه طریقی به حساب بانکی مردم ایران دسترسی پیدا می کنند و برای این امر دقیقاً به چه اطلاعات اولیه نیاز دارند؟!

**ELECTRA H** بدو بیارید بازیابی بزنم 7:23 PM 3

**ELECTRA** بدو بیارید بازیابی بزنم 7:27 PM

**ELECTRA H** برا بازیابی چه اطلاعاتی نیازه؟ 7:28 PM

کد ملی  
ش تلفن  
ش کارت

**Lord | خدا** برا بازیابی چه اطلاعاتی نیازه؟ 7:28 PM

**ELECTRA H** کد ملی داشته باشی بقیش درمیارم 7:28 PM 1 Reply

**ELECTRA** ...کد ملی داشته باشی بقیش حله 7:29 PM

آیا می دانستید که اینگونه افراد تنها با دانستن کد ملی شما، براحتی قادر هستند سایر اطلاعات مورد نیاز را بازیابی کرده و به حساب بانکی شما دسترسی و دست درازی کنند؟



دادستانی کل کشور  
معاونت پیگیری امور قضای مجازی

تاریخ: \_\_\_\_\_  
شماره: \_\_\_\_\_  
پیوست: \_\_\_\_\_

استفاده از رمزهای ایستا در این فرآیندها است که موجب شده مجرمین با بدست آوردن رمز دوم و اطلاعات کارت قربانی، به راحتی بتوانند از حساب بانکی بزه دیده برداشت نموده و یا از فروشگاه های اینترنتی خرید نمایند.

اطلاع رسانی صداوسیما و سایر مراجع ذیصلاح در خصوص اجرایی شدن بکارگیری رمزهای پویا باعث گردید، اطلاعات کارتهای بانکی مردم که در طول سالیان گذشته از طریق درگاه های پرداخت جعلی و فیشینگ در اختیار مجرمین قرار گرفته بود، با نزدیک شدن به موعد اجرای رمزهای پویا (۹۸/۳/۱) در ابعاد بسیار گسترده و فراگیر توسط مجرمین سایبری مورد سوء استفاده قرار گیرد.

این آمار فرآیندهای بانکی وضعیت بحرانی رشد این جرایم در کشور است به نحوی که فقط در تهران بطور روزانه حدود ۲۰۰ فقره پرونده جدید ثبت می شود و صرفاً در خردادماه سال جاری بیش از ۲۴۰ میلیارد ریال خسارت مالی وارده به بزه دیدگان این جرایم بوده است. (این آمار صرفاً مربوط به آمار یک ماه برداشت غیرمجاز از حساب یا مبالغ بالای ۵۰۰ هزار تومان و براساس پرونده های ارجاع شده به پلیس فتا بوده است و با احتساب تخمین مشابه از سایر ماه های سال و لحاظ جرایم زیر ۵۰۰ هزار تومان و باتوجه به اینکه بسیاری از جرایم خرد بدلیل طولانی بودن فرآیندهای قضایی اساساً مورد شکایت قرار نمی گیرد و برخی دیگر از این شکایات در پلیس آگاهی به ثبت می رسد، آمار واقعی این جرایم و خسارات وارده دهها برابر بیشتر از آمار اعلامی خواهد بود.)

ضمناً براساس تخمین پلیس فتا اگر این وضعیت ادامه پیدا کند در پایان سال جاری حدود ۱۸۰ هزار تا ۶۰۰ هزار نفر از مشتریان بانکی، متأثر از این جرایم شده و علاوه بر اینکه هزینه های هنگفت مادی و معنوی به بزه دیدگان، دستگاه قضایی و ضابطان دادگستری تحمیل خواهد کرد، ممکن است موجب ایجاد تبعات اجتماعی و امنیتی و نارضایتی گسترده در جامعه شود.

علاوه بر موارد فوق عواید مالی ناشی از برخی دیگر از جرایم نظیر سایر کلاهبرداری های رایانه ای و قماربازی های اینترنتی نیز از طریق کارت های بانکی که اطلاعات ایستای آن ها از طریق فیشینگ در اختیار مجرمین قرار گرفته است تبادل می شود و چنانچه بخشنامه بانک مرکزی مبنی بر استفاده از رمزهای پویا اجرایی نشود، سوء استفاده از کارت های بانکی اشخاص در دیگر جرایم فضای مجازی نیز رشد چشمگیری خواهد داشت. براساس گزارش پلیس فتا، گردش مالی قمارخانه های آنلاین در سال گذشته به رقم ۲۲۰۰ میلیارد تومان بالغ شده است و پیش بینی می شود بیش از یک میلیون و دویست هزار نفر در کشور به این جرایم آلوده شده باشند.

یکی از مهمترین دلایل من برای جمع‌آوری آن همه اطلاعات هویتی نشت پیدا کرده از هک‌های اخیر ، بررسی ابعاد مختلف و نشان دادن تهدیدات احتمالی یک فاجعه بود. فاجعه‌ای که بدون این دیتاها کسی حاضر به پذیرش آن به این راحتی‌ها نبود و با دیتا نیز که خودتان از نزدیک شاهدش بودید و تجربه‌اش کردید 😞

The collage consists of several parts:

- Top Left:** A handwritten document in Persian with the title "بهبشتی!" (Behbeshi!). The text discusses the risks of digital identity theft and the importance of protecting personal information.
- Top Right:** A Telegram chat interface showing a discussion about a loan from "قرض الحسنه مهر ایران" (Mehregan Loan). The chat includes a "Discussion started" notification and several replies.
- Middle Left:** A Bank Sepah credit card with the number 1015 4928 and the name "شبا: 5012".
- Middle Right:** Another Telegram chat showing a discussion about "Coin Digital" and "اتحاد فیش" (Atahad Fesh).
- Bottom:** A red banner with white text warning about the dangers of identity theft and the importance of protecting personal data.