سالانه 12.6 میلیون نفر از مردم جهان قربانی سرقت هویت آنلاین شده و بیش از 21 میلیارد دلار ضرر مالی می بینند.

این مشکل بزرگ به نوشته کمپانی امنیتی هات اسپات شیلد، حل نمی شود مگر اینکه کاربران بدانند چگونه هکرها وارد می شوند و اطلاعات شخصی و کسب و کارشان را به سرقت می برند.
اینفوگرافیک زیر سعی می کند راههای ورود هکرها و اشتباهات قربانیان که منجر به سرقت اطلاعات می شود را بررسی کند.

چه نوع دیتایی مورد حمله هکرها واقع می شود

هکرها دنبال چه هستند؟

مهمترین دیتایی که در سال ۲۰۱۱ و ۲۰۱۲ در اولویت حملات هکری بوده: اطلاعات دارنده انواع کارتهای بانکی و اعتباری بوده است.

98% استفاده ۹۸ درصدی از کارتهای سرقتی در امور کلاهبرداری و نقل و انتقال های غیر قانونی

1% شماره حساب و اکانت های بزرگ مالی

1% اطلاعات کارتهای هوشمند سلامت

2% اطلاعات محرمانه و مالکیت های معنوی

دلیل استفاده از اطلاعات بانکی دیگران توسط هکرها، شناسایی هویت سارقان است که بدین ترتیب هکرها از شناسایی شدن فرار می کنند و ماموران به در بسته می خورند

12.6 MILLION

تعداد قربانیان هک کارتهای اعتباری در سال گذشته
هر سه ثانیه یک قربانی

$21 BILLION

۲۱ میلیارد دلار خسارت بابت سرقت اطلاعات کارتهای اعتباری

چک لیست یک هکر

- شماره مجوز گواهینامه ها و مدارک حرفه ای
- شماره حساب بانکی و کارتهای اعتباری
- نام کاربری،پسورد و شماره پین
- شماره بیمه های مختلف
- شماره دانشجویی و کارمندی
- شماره رفاه اجتماعی
- شماره تسهیلات دانشجویی
- شماره گواهینامه و شماره پاسپورت
- شماره تلفن و قبوض

راههای ورود یک هکر

چگونه یک هکر مرا پیدا می کند؟

هکرها راههای مختلفی برای سرقت اطلاعات و دیتای شما دارند

مختصات فنی

47%

۴۷ درصد با روش دسترسی به دیتا از راه دور

26%

۲۶ درصد با تزریق کد اسکیوال به وب سایت و سرقت دیتا

18%

۱۸ درصد با روش های ناشناخته دیتا ها را سرقت کرده اند

3%

۳ درصد با روش اجرای کد و دستورات مخصوص از راه دور روی سرور

2%

دو درصد با روش حمله به سیستم نفوذ پذیر کاربری که وب سایتی را مرور می کند

2%

دو درصد با روش ارسال فایل از طریق اسکریپت نوشته شده روی وب سرور

2%

دو درصد با روش فعل و انفعالات کاربری و نوع حرکت و کلیک کاربر روی محتواهای خاصی که باعث دسترسی به اطلاعات بانکی می شود

1%

یک درصد با روش کشف رخنه در "اجازه قانونی دسترسی" و دسترسی به فایلها و اطلاعات با بداقزار

1%

یک درصد به روش سرقت فیزیکی کامپیوتر یا کارت اعتباری از شخص به صورت مستقیم

شبکه های اجتماعی

بکار بردن اطلاعات شخصی صحیح در پروفایل سایتهای شبکه های اجتماعی توسط کاربران، منبع خوبی برای هک کردن دیتا محسوب می شود تا با استفاده از نام فرزندان و همسر و تلفن و شماره های ... آسیب پذیری و قرار گرفتن دیتای بانکی برای هکرها آسان تر شود

۱۶ درصد از دانشجویان قربانی فریب های کنترل شده فیشینگ می شوند. در حالی که ۷۲ درصد از قربانیان از طریق ایمیلهای ناخواسته دوستان قربانی لینک های کلاهبرداری و سرقت دیتا می شوند.

۶۸ درصد از مردم در پروفایل عمومی شان، تاریخ تولد خود را ذکر می کنند

۱۸ درصد شماره تلفن خود را می نویسند

۶۳ درصد نام دبیرستان خود را می نویسند

۱۲ درصد نام حیوان خانگی خود را می نویسند

تمام این موارد هنگام سرقت اطلاعات ممکن است توسط هکرها استفاده شود

HOTSPOTS

یک هکر اتصالات هات اسپات تحت نام فرودگاه، کافی شاپ و ... می سازد و شما با لپ تاپ به آن وصل شده و اطلاعات تان را به سرقت می برد.

89%

۸۹ درصد از هات اسپات های بی سیم همچنان نا امن هستند.

HOME WIFI

یک هکر در همسایگی شبکه بی سیم خانگی شما ممکن است به اطلاعات شخصی شما دست یابد. بهترین کار استفاده از انتخاب حمایتی **WPA**-۲ است.

19%

اما ۱۹ درصد از قربانیان شبکه های بی سیم از رمزگذاری های **WEP** که ناامن هستند، استفاده می کنند.

وب سایت های مشکوک و مظنون

هکرها از متد تزریقی **SQL** برای جمع آوری اطلاعات شخصی از فرم های کاربری تعریف شده، استفاده می کنند.
وب سایتهایی با جستجوهای جعلی و مملو از بدافزار تا به هکرها اجازه دانلود دیتای شخصی کاربران را بدهد

۴۸ درصد از تحقیقات مربوط به

48%

سایتهای تجارت الکترونیک می شود

EMAIL

هکرها بعد از جمع آوری ایمیل ها، از طریق شخصی که شما وی را می شناسید وارد می شوند

10%

۱۰ درصد از پیام های اسپم، مظنون فعالیتهای هکری است

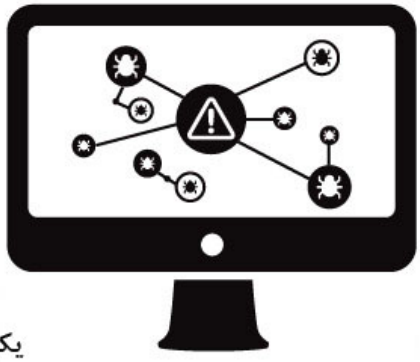
7%

۷ درصد از اسپم ها آلوده به لینک های هکری است

کشف و ردیابی

چگونه هکرها بدام می افتند؟

هکرها پیچیده ترو پیشرفته تر شده اند و راه حل های اکتشافی و خنثی سازی علیه آنها مانند برنامه های ضد ویروس کارآیی خود را از دست داده اند. بعلاوه بدافزارها چراغ خاموش می آیند و این در حالی است که چشمان شما از حدقه بیرون زده است.



48%

۴۸ درصد از کشفیات به صورت عادی متحقق می شود.
یکی از راههای عمده مبارزه با هکرها همچنان تکنیک های دفاعی تعریف شده عمومی است

25%

۲۵ درصد از کشفیات توسط فشار قانونی و آژانس های قضایی در مبارزه با جنایات سایبری بدست می آید

24%

۲۴ درصد کشفیات توسط خود کاربر انجام می شود

دفاع

چگونه می توانم از خود و سیستم ام در برابر هکرها محافظت کنم؟

امن کردن پسوردها

بیش از ۶۰ درصد کاربران

60%

از یک پسورد برای چند سایت استفاده می کنند

پسورد سخت و منحصربفرد با ترکیب شماره ها، حروف بزرگ و کوچک و کارکترها بسازید

از نام حیوان خانگی خود یا سال تولد برای پسورد استفاده نکنید

امن کردن مرورگر

هرگز اطلاعات شخصی خود را به اشتراک نگذارید مگر اینکه از پروتکل اچ تی تی پی اس استفاده کنید.
همیشه از صفحه خود بیرون بیایید/ لاگ.آوت کنید

44%

۴۴ درصد از مردم نمی دانند چگونه از دیتای شخصی خود محافظت کنند

وقتی شما لاگ.آوت نکرده و از سیستم خود بیرون نیایید، راه را برای ورود غیر قانونی هکرها باز گذاشته اید

امن کردن شبکه

روی ویندوز **Autorun** را غیر فعال کنید

50%

تا جلوی ۵۰ درصد تهدیدات بدافزاری را گرفته باشید

دیفالت تنظیمات امنیتی معمولا اجازه ورود هکرها به سیستم شما را می دهد.
همیشه تنظیمات را به نحوی که می دانید با هدف امن تر کرده، تغییر دهید.

بدافزار از طریق لینک دانلودی که شما ناگهان می بینید وارد می شود

Hotspot shield VPN service enables you to surf the web anonymously and securely, protecting you from hackers, malware, and identity theft. **Get hotspot shield for free at www.hotspotshield.com.**

Sources

http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf
http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp
http://www.techrepublic.com/blog/security/dropsmack-us
ing-dropbox-to-steal-files-and-deliver-malware/9332?tag=nl.e101&s_cid=e101&ttag=e101
https://media.blackhat.com/eu-13/briefings/Williams/bh-eu-13-dropsmack-jwilliams-wp.pdf
http://lifehacker.com/5938980/how-secure-are-you-online-the-checklist
http://www.splashdata.com/press/PR121023.htm
http://www.zdnet.com/blog/security/survey-60-percent-of-us
ers-use-the-same-password-across-more-than-one-of-their-online-accounts/9489
2013 global security report
https://we.riseup.net/riseuphelp+en/how-vpn-works

منبع :[خبرآنلاین به نقل از هات اسپات شیلد]