

The Cost of Our Email Identity for Cyber Criminals

Putting a price on your digital identity

SLIVEN, BULGARIA, January 14, 2019 /EINPresswire.com/ -- What do your hotel loyalty card, your online bank account and your email inbox have in common? They are all very valuable to cyber criminals! This blog post explores the many ways in which hackers are trying to make a profit of your online accounts. Make sure you are aware of their methods, so you can [defend yourself when your digital identity is under attack](#).



BULIDSEC Email Identity Guard

Whether you upload photos to your Facebook profile, book a hotel room online or send private emails using your webmail provider - your online identity contains both valuable memories and valuable data. The fact that cyber criminals are interested in these accounts should therefore not come as a surprise. The more sensitive data is processed online, the higher the potential profit is for criminals. For example, hacked iTunes accounts have been reported to sell for \$8 a piece on underground markets - because hackers can use them to buy products and services with the associated credit card details. Similarly, McAfee reported a selling price between \$0.55 and \$15 for accounts for online video streaming services, which can be sold on to unscrupulous users looking for a cheap deal on video content.

Interestingly, even accounts for services that can be used at no cost represent a very real value to cyber criminals. The McAfee report quotes a selling price of \$20 for hotel loyalty accounts - which are free for hotel guests that enroll into a loyalty program. Because customers can use loyalty cards to save up points for free hotel stays, they become a target for criminals who redeem the points themselves or sell them on to others. Similarly, online auction accounts, which can typically also be created for free, are popular with cyber criminals. By stealing the digital identity of a seller with positive ratings on an auction platform, they can hide their own reputation when selling fraudulent services or products.

A popular approach to stealing digital identities is phishing. When an online service becomes victim of a data breach, criminals try to extract whichever data they can. If they can get hold of customer email addresses, they often contact users directly and try to impersonate the service in order to extract more information, or even money, from the victims. For example, when criminals obtain email addresses of online banking customers, they may set up a fake online banking website. By luring customers to the fake website, they can intercept login data, which can then be used to steal funds from the account. Some data breaches contain even more data, such as user names and passwords. Cyber criminals that manage to steal such data do not even need to turn to phishing. Instead, they can directly abuse the login data and for instance reuse your identity to attack the accounts of your contacts. For customers that reused their login data

on other websites, the effects can be even more damaging, as the criminals are now able to log in to their accounts across the internet.

Considering that the number of active email accounts worldwide is expected to reach 6 billion by 2019, the number of potential targets for phishing and other methods of identity theft will only increase. This means that it is getting ever more important to [protect yourself against digital identity theft](#). BULIDSEC offers a unique software tool that helps you monitor in real time your email identities. [BULIDSEC Email Identity Guard](#) makes sure that you are immediately notified if your email address is leaked after a data breach. It lets you take appropriate countermeasures quickly so that cyber criminals can not take over your digital identity!

Petko Ganev
BULIDSEC LTD
[email us here](#)
+359 888676836

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2019 IPD Group, Inc. All Right Reserved.