BullGuard offers security advice to those affected by password hacking

Submitted by: The PR Room
Friday, 8 June 2012

LinkedIn, eHarmony and Last.fm targeted, phishing attempts on stolen passwords begin

London, 8th June 2012: Internet security expert, BullGuard (http://www.bullguard.com), has reacted to the theft of millions of user passwords from the popular business-based networking site LinkedIn, dating site eHarmony and now Last.fm, encouraging individuals to be more vigilant with their online security (http://www.bullguard.com/products/bullguard-internet-security-12.aspx).

A year after the high-profile Sony Playstation Network security breach, LinkedIn users were recently informed that 6.5million user account passwords had been stolen and published on a Russian computer hacking forum, leaving them open to phishing attacks and potential infection by malware designed to steal personal data from a host computer. Since then 1.5million passwords were stolen from online dating site eHarmony and music website Last.fm is the latest to announce a breach of its security. These attacks have already yielded a number of phishing scams – hackers are targeting those affected by the LinkedIn hacking (http://www.bullguard.com) with fraudulent emails that appear to be official correspondence but direct to a website selling counterfeit drugs.

The frequency at which these attacks took place would suggest that associated parties are involved, or at least that a common vulnerability is being exploited in order to retrieve these large numbers of user data. The number of affected users could also be far higher than predicted, according to security analyst Imperva, who believes that the numbers tallied so far do not take into account duplicate passwords, leading to calls to revisit security measures on such websites and for users to be more careful with their sensitive data.

Claus Villumsen, CTO at BullGuard, reiterates the need for modern internet users to look after their own interests rather than relying solely on the security measures of a third party. “We’d all like to believe that our personal details and sensitive data are being kept safe from prying eyes when signing up to a service from reputable companies such as those affected,” he states. “The reality today, unfortunately, is that this is not the case. Hackers are renowned for moving quickly to find ways around modern security measures, and consumers should be vigilant to these concerns and always assume that the first step towards keeping sensitive data safe lies with them.”

LinkedIn has already advised users to ignore any emails requesting information and instead to log in to the site directly to change their LinkedIn password, a message that has been echoed by eHarmony and Last.fm. However, the recent attack and possibility that more are to follow should prompt many to reconsider the types of sensitive data they keep stored on their accounts. BullGuard encourages safe and proper password use to help reduce the risk of being targeted, and suggests that users consider the more wide-reaching impact of their account data being stolen.

In reaction to the recent attacks:

• Users should change the username and passwords for unrelated accounts that use the same username

and/or password as the affected account. As most people use the same few passwords/security questions for all their accounts, stolen passwords pose a major security risk.

• Change security questions and password on accounts where possible.

• Avoid social media applications that ask to access your personal information to allow you to continue.

• As much as possible, limit the personal information that you make public on social media websites.

• Only download applications that are provided by a trusted source.

• Be suspicious of any e-mails that request your personal information no matter how legitimate they may seem.

General advice on how to protect personal details on public networks:

• Familiarise yourself with the security settings and ensure that an account doesn't reveal too much information to users that haven't been approved to view it. Also consider whether the information you store online really needs to be there, or whether it could be potentially used for fraudulent activity if read by a malicious third-party.

• Do not store credit card details online. Many services have so-called "e-wallet" services which allow users to store credit card details, in order to make future purchases fast and easy. This conflict between security and convenience is a huge dilemma for online services, and should be something end users consider carefully as well.

• Do not use the same passwords and security questions for all accounts. Most people alternate between 2 or 3 passwords for everything. Consequently, if one account is hacked, identity thieves have access to all different profiles and accounts. Ensure that passwords and security questions used for banking and money transfers are very different from the ones used elsewhere.

• If users mention a child's, pet's or spouse's name on social media sites like Facebook and Twitter, do not use these for passwords.

• Only make purchases with devices that have security software (minimum antivirus and firewall) installed such as a home or office PC.

• Always ensure that security software (http://www.bullguard.com/products/bullguard-internet-security-12.aspx) is up to date.

General advice on safe password use:

• Choose safety over convenience - Since there are so many websites around that require login and password details to access a user account it's all too common to see people adopting straightforward,

easy to memorise passwords that could simply be “guessed”. A survey by data security firm Imperva analysed 32 million passwords to find the top-ten most commonly used. Five of the top ten were simply sequential digit strings such as “123456”, with the remaining including “password” and “abc123”.

• Avoid personal information, such as a mother’s maiden name, favourite pet, birthplace or date of birth when choosing a password. This sort of information is frequently used to confirm authenticity with online banks and services, and could therefore be subject to keylogging and phishing scams.

• Use a combination of letters and numbers in a password as well as a word that would be very difficult for a third-party to guess. With a bit of practice it becomes almost second nature to tweak common words in this way to generate a more difficult to predict phrase.

• Change passwords as often as possible, particularly in the case of sites that involve frequent or large monetary transactions such as bank accounts, online payment services and commonly used e-retailers. However, it’s not usually a good idea to “rotate” a handful of passwords around as hackers can quickly build a list of common words and phrases if they have gained access to a computer.

-ENDS-

More information:
Press Contact

Sarah Chard
The PR Room Ltd
Tel: 0845 094 2902
Mobile: 07779 584 799
sarah.chard@theprroom.co.uk

About BullGuard:
Launched in 2002, BullGuard is one of the fastest growing security brands. Its philosophy has always remained the same - to combine technical excellence with a genuine understanding of consumer needs, creating simple, easy to use products that deliver universal, complete protection as well as enabling customers to control and manage their digital footprint.