3 Lessons Learned from the LifeLock Bug

A lot of people (4.5 million) depend on LifeLock, a subsidiary of security giant Symantec, to help them protect their online identity. Ironically, the company recently admitted that a vulnerability on the LifeLock website had potentially exposed millions of customer email addresses to hackers.

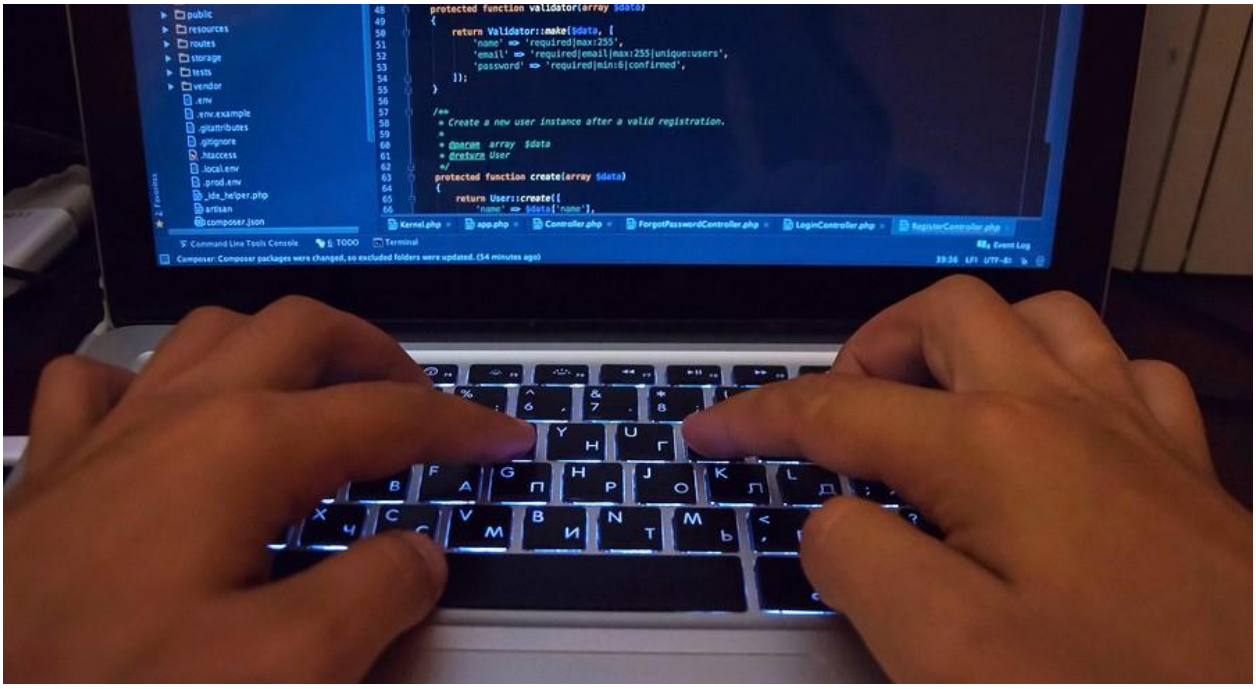
This all sounds familiar. Remember the Equifax security breach fiasco? Or, more recently, a website breach at Panera Bread? In each case, unauthorized persons were able to access millions of customer records through the company website. These incidents and dozens more serve as cautionary tales for organizations and consumers alike.

What Happened at LifeLock

On July, a security researcher attempted to unsubscribe from marketing emails sent by LifeLock. In the process, he discovered that an error on the marketing opt-out page would allow him to easily obtain email addresses for millions of LifeLock customers.

Imagine the mass phishing campaign a bad actor could launch with the email addresses of customers known to have identity theft concerns. By playing on their fears of losing protection, a phishing campaign could trick users into making payments through a fake site.

In this case, it appears that the web page that contained the bug is managed by a third party. LifeLock quickly fixed the problem, but the possible exposure of sensitive data teaches some practical and essential lessons.



Lesson 1: Safe Website Development is a Must

Any organization that stores personal data from its customers, even information as simple as an email address, has a responsibility to keep that data secure. Websites are a particularly vulnerable target for hackers.

Consider all the personal data that customers provide through a website. They enter financial and mailing information to order products online. They list account identifiers and social security numbers. Or, they specify personal preferences and a birthdate as they sign up for a customer loyalty program.

Creating a bulletproof website is extremely challenging. But when you have customer and company data at stake, you cannot afford to take shortcuts with security. Take the time to adopt a security policy that addresses potential vulnerabilities within your website development process. In addition to coding specifications, this will include items such as the following:

- Use strong passwords for your server and website administration areas. Enforce secure passwords for your users. Always store passwords as encrypted values.
- Use HTTPS for your entire site. In fact, some browsers mark any site not protected with an SSL certificate as "insecure."
- Conduct penetration testing regularly to expose potential issues with your website security.
- Keep all your software up-to-date, applying security updates promptly.

Lesson 2: Keep an Eye on Your Partners

The unsubscribe page that allowed access to LifeLock customer email addresses is apparently maintained not by LifeLock, but by an outside business partner. Still, at the end of the day, customers trust their data security to the company whose name displays at the top of the website.

You cannot assume that third parties that impact your site have airtight security practices in place. Police not only your own web framework, but also the activities of your partners. Regularly scan their sites to identify vulnerabilities.

Lesson 3: Protect Your Own Personal Data

While you protect personal data provided by your customers, remember to safeguard your own digital identity. Change your passwords frequently. Understand and use available privacy settings. Avoid public Wi-Fi and online quizzes. Think twice before you share sensitive personal information on social media.

Online shopping and the endless amount of data available on the internet have brought the world literally to our doorsteps, Unfortunately, all that convenience can make consumers complacent. Remember that it is much more effective to practice safe computing than to try and repair a stolen identity.

Security without the Fuss

Staying on top of emerging threats and potential vulnerabilities up and down your supply chain requires significant time and resources. A trusted partner with proven experience in security management can help you secure your website and safeguard sensitive data.

The professionals at eMazzanti Technologies offer customized security solutions and award-winning website design. Since 2001, eMazzanti has delivered world class solutions that protect sensitive business data, so you can focus on your core business.