Payroll Site Hack Swells Employment Rolls

By Kim Zetter ✉ October 16, 2009 | 2:11 pm | Categories: Breaches

A payroll-processing firm that was breached by hackers last month is warning customers about a new breach, after some clients noticed phantom employees popping up on their payrolls.

New Jersey-based PayChoice sent a message to customers Thursday indicating that thieves appeared to have stolen customer login IDs and passwords by exploiting a vulnerability in the website feature for changing a password, WashingtonPost.com reports. PayChoice said it disabled the change-password feature until it could fix the vulnerability.

The company discovered the problem after some of its payroll customers noticed bogus employee names being added to their payroll lists, in an attempt to get the companies to pay those "employees" through bank accounts controlled by the fraudsters.

The incident follows a breach in late September that resulted in hackers absconding with the account information of firms using its online payroll product.

In a Sept. 28 e-mail sent to customers, PayChoice indicated that the hackers had obtained e-mail addresses as well as login IDs and at least parts of passwords for account holders using the OnlineEmployer.com website.

The hackers used the information for a phishing attack, sending targeted e-mail to the customers in an attempt to trick them into relinquishing the remainder of their passwords. The e-mails indicated that the customers needed to download a plug-in to continue using PayChoice's OnlineEmployer website. The plug-in, however, was actually a password-stealing Trojan.

PayChoice shuttered the site temporarily after discovering the initial attack, and, in an attempt to beef up security, forced customers to change their passwords.

In addition to its payroll-processing service, PayChoice produces an online payroll-management system used by 240 other payroll processing firms,

See also:

- Payroll Firm Breached — Online Customers Targeted

Post Comment | Permalink

Comments (5)

Posted by: SBMfromLA | 10/16/09 | 8:51 pm |

It makes me wonder if any of their customers ever needed any type of plug-in to use their services.. and if not, the Login screen for their customers should always caution about fraud and about never giving out their passwords. If a simple warning was always present on the login screen with simple warnings.. it seems the customer would be able to protect their accounts better.. and if they were redirected to a fake web site, they would know something was up if the login screen's "warnings" were suddenly gone and a message appeared about installing a plugin or giving out a password…

I hope that made sense… hahaha

Posted by: TheLifehackPost | 10/17/09 | 11:49 am |

If a simple warning was always present on the login screen with simple warnings.. it seems the customer would be able to protect their accounts better.. and if they were redirected to a fake web site, they would know something was up if the login screen's "warnings" were suddenly gone and a message appeared about installing a plugin or giving out a password. (Mimeblogger

---

Posted by: Nym | 10/18/09 | 3:24 am |

Well, it probably caught their eye when a check started to roll for "Blingy Cashopolous" or any one of a billion other silly spam names these clowns tend to use.

Posted by: tthomas48 | 10/19/09 | 3:32 pm |

The real question is why exactly anyone would be able to get "at least parts of passwords for account holders". They should be storing them as one-way hashes so there's (almost) zero chance of this happening. That detail alone makes me really doubt their security.

Posted by: jing123 | 11/19/09 | 4:06 am |

links banglesits very good information thanks
