

March 2004

Local Cyber-hero Frederic Bitwayiki discovered a web site last weekend that accidentally exposed MasterCard and Visa card numbers. MasterCard and Visa were immediately contacted and the site is now secure.

Frederic works for Channel 27 in Madison. After seeing a commercial for a buy-over-the-web product, Fredrick went to their website to learn more about it. While there, he noticed menus just like the ones you see when installing a web server. Amazingly, the merchant had installed the web server but had never changed the default administrator's name or password. Worse yet, the merchant was also storing full credit card numbers directly in their database.

We don't know how long the customer list was exposed. It contained complete information on every customer, including name, address, credit card number, CW2 card code verification, and expiration date.

Frederic called me and we immediately notified Citibank Visa's Suspicious Merchants Department. They then notified Visa and MasterCard Security. The merchant was surprised that there was a problem and reacted by saying that they simply used the password they were told they must use. After some merchant education, the merchant learned that it is a good idea to change the password before deploying the software. And the credit card companies have specific guidelines about securing and disposing of credit card numbers.

The security departments are somewhat tight-lipped about the actions they take, but they have assured us that the exposure was closed and that appropriate actions have been taken to watch the activity of any credit cards that were at risk.

Channel 27 aired a story on the case. Congratulations to Frederic for noticing the breach and reporting it immediately.

/Jim Gast

Jim Gast, gastj@uwplatt.edu
Computer Science and Software Engineering
512 Pioneer Tower
Platteville, WI 53818