



PHARMING:



Is Your Trusted Website A Clever Fake?

What is Pharming?

Pharming is a term for when criminal hackers redirect Internet traffic from one website to a different, identical-looking site. Pharming occurs when you key an address into your Internet browser. Instead of going to the legitimate site, you are redirected without your knowledge, to a fake site. This is done in order to trick you into entering your user name and password into the database of their fake site.

Criminals try to acquire your personal information in order to access your bank account, steal your identity, or commit other kinds of fraud in your name, so banking and similar financial sites are often the targets of these attacks.

Protect yourself from Pharming Scams

- Always use a secure website when you submit credit card or other sensitive information via your Web browser. The beginning of the Web address in your browser address bar should be “https://” rather than just “http://.”
- To protect your financial information, login to Internet Banking often and review your transaction history. Notify the Customer Service Department of any suspicious transactions.
- Check your credit and debit card statements to ensure that all transactions are legitimate. If anything looks suspicious, contact the Bank and all card issuers immediately.
- Regularly check that your browser is up to date and new security patches are applied.

Rest assured the Bank is taking every precaution to protect your safety. To help prevent identity theft the Bank diligently manages domain names by ensuring that the domain names are renewed in a timely manner. The Bank also investigates the possibility of registering similar domain names.

If you fall victim to pharming, act immediately to protect yourself, contact the Bank’s Customer Service Department at (877) 226-5820 and alert them to the situation.

Visit the Bank’s Customer Center page at www.bankecc.com/ECC_Customer_Center.htm for more consumer safety information.