MTBN.NET PLR Library
Category: Finance File: Encrypted_Email_--_Users_Unknowingly_Put_Banking_Data_at_Risk_utf8.txt
Text and Word PLR Article Packs available at PLRImporter.Com

Title:
Encrypted Email -- Users Unknowingly Put Banking Data at Risk

Word Count:
596

Summary:
PGP is one of the most common methods of protecting financial data that customers submit through banking and financial websites.

Keywords:
banking data, financial data,pgp

Article Body:
PGP is one of the most common methods of protecting financial data that customers submit through banking and financial websites. PGP provides excellent data encryption, but many users leave sensitive PGP-encrypted data vulnerable without even knowing they’re doing so.

Banks, credit unions and other financial institutions use PGP to encrypt sensitive data, such as a loan application, before sending it through email. PGP makes the data is nearly impossible for anyone other than the intended recipient to decrypt. Unfortunately, after receiving the data the recipient often unknowingly creates an opportunity for thieves to steal the data.

Recipients decrypt PGP protected email messages to read the sensitive contents. Security-savvy users know to that after reading the message they need to either permanently delete the encrypted message or to save it in its original encrypted state. But a large number of users in financial institutions that we’ve worked with don’t do either. Instead they save the decrypted version of the email where thieves can easily access the information. In fact, Microsoft Outlook prompts users to save encrypted messages in a decrypted form whenever they close a decrypted message. Since neither Outlook nor PGP warns users about the danger of saving the message, most users click “Yes” and save the decrypted message.

When decrypted, the data is vulnerable to attack by viruses, malware and computer hackers. Some executives dismiss the threat by touting the protection that their firewalls and intrusion prevention systems provide. Firewalls are almost useless when PCs are infected with data harvesting viruses or malware, so relying on firewalls to protect data stored on PCs is akin to putting a lock on a screen door.

MTBN.NET PLR Library
Category: Finance File: Encrypted_Email_--_Users_Unknowingly_Put_Banking_Data_at_Risk_utf8.txt
Text and Word PLR Article Packs available at PLRImporter.Com

Even when firewalls do manage to keep PCs free of any viruses or malware, what happens when the bad guy is someone inside the organization?

According to the FBI, insiders – employees, contractors and business partners – commit nearly 70% of all data theft crimes. They steal data directly from the corporate network or they steal the computers & hardware that store the data. Sometimes they even "buy" the data by purchasing decommissioned computers that organizations sell to employees. A firewall will do nothing to protect decrypted data stored on the PCs that these attackers gain legitimate access to.

We've implemented a safer way to protect data submitted through websites. Using MemberProtect, our clients have eliminated the decrypted data theft risk. MemberProtect does not rely on email delivery and instead stores data inside a uniquely-encrypted database. Administrators control who can access the secure web-based viewer to see the data submitted through their websites. MemberProtect decrypts the data to allow viewing, but unlike Outlook, MemberProtect always re-encrypts the data when the user is done viewing it.

MemberProtect also creates an audit trail that auditors and security administrators can use to see who has viewed, modified and deleted data. It also tracks logons, attempted logons and user interactions with the protected system. MemberProtect stores this audit login a separate encrypted database to prevent log tampering by system administrators or other insiders. When integrated with intrusion detection systems, the system can perform a degree of self protection by severing connections with suspicious clients and immediately notifying administrators of suspected hack attempts.

If your budget cannot support a system like MemberProtect (approximately $3,000 to $5,000 for implementation on a bank website), then PGP is still an acceptable security option, but it's critical that you train all users to:

Never save decrypted messages
Never share their PGP pass phrase
Always make a backup of their private key since if this key is lost, the messages cannot be decrypted