# Email Encryption Unlocked

cyber security encryption

Secret decoders have been available for many years as a fun way for children to wet their appetite for ciphers, codes and encryption. Starting in the 1930s, simple decoders were frequent giveaways. At the time, secret decoder pins were the norm, followed decades later by secret decoder rings. Nowadays, there are secret decoder wheels, kits, glasses, printable code games and more. Whatever the medium, kids are as fascinated today as they were decades ago with the idea of uncovering secret messages. Adults, too, can continue to enjoy the fun with items such as obfuscated business cards.

Encoding messages also has a more serious application these days in banking however, given an uptick in cybercrime. To help protect sensitive information, community banks are beginning to turn to encrypted email for instance to help protect basic communications. To be sure, most customers don't think twice before they send personal information in an email. That is scary when you consider one study found it takes about 15 minutes only for the bad guys to break in. People are so crazy, they even send emails with such sensitive data as a Social Security number, bank account or credit card number. Many people just don't seem to understand the potential for harm if these sensitive numbers fell into the wrong hands.

The reality is that without encryption, there's nothing stopping a third party from intercepting and reading your email messages. Even email providers troll through your messages from time to time to identify pertinent advertising opportunities. Meanwhile, an increasing number of industry, state and federal regulations require the encryption of sensitive data. The FFIEC's examination handbook, for instance, says financial institutions "should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit." FFIEC doesn't specifically mention email, but some banks are nonetheless adopting the use of encryption for all outgoing emails.

Certainly, there are challenges when using email encryption. For instance, it typically adds another step to what is currently a seamless process of communication. Adding encryption can bog things down and users aren't keen to add in more data and remember more passwords just to secure what seems to be something so simple and easy to use.

Consider though research by ZixCorp on this subject. It cites information from Osterman Research that finds the average person spends 146 minutes per day in email vs. 54 minutes on the phone, 23 minutes using instant messaging and 18 minutes on social networking sites. It also found a whopping 25% of all email messages contain attachments.

There are certainly a number of different providers of email encryption services, but they aren't all created equal, so you'll have to do your homework to find a partner that best fits your needs. When researching

providers, take into account factors such as the method of encryption, how seamless the user experience is, the ease of day-to-day administration and the provider's credentials and track record.

If customers find communicating through encrypted email too difficult to use, it will be a barrier to doing business with your bank, so you'll need to tread especially carefully here. Another problem could arise if bank employees even occasionally use their personal, unsecured email, to circumvent an encrypted bank email system that's overly complex and not user-friendly. Moreover, if a solution doesn't offer you the protections you're seeking, then it's an added cost with very negligible benefit.

In time, it's likely that email encryption will become more popular as the hackers continue to break into systems, so it may be a good time to take a look at your options. If nothing else, you'll generate a healthy dose of nostalgia for childhood spy games.