

Increased threats from phishing forces companies to restructure their customer communications

~ E-mail signature seen as one solution, but according to TC TrustCenter, only few companies inform their customers about new options for secure mail dialoguing ~

Hamburg, November 28, 2006. The number of phishing attacks keeps rising unabated: Whereas the Anti-Phishing Working Group (APWG) logged just under 12,000 phishing websites active online in May, in July that figure had jumped to 14,191 – with the upward trend continuing. In Germany the damage caused by such attacks was around 5 million Euros*. One conspicuous aspect of the current trend is that both the phishing websites as well as the fraudulent e-mails that originate from them are becoming more and more professional, and appear deceptively authentic. As a result of this alarming development, certain industries including the banking and financial sectors can hardly employ e-mail as a communication tool anymore without the recipients doubting its authenticity. Employing an e-mail signature is currently the most secure method: According to TC TrustCenter, however, while many companies already actively protect their employees against phishing, they neglect to inform their customers about the security measures in use. The German-based specialist for digital certificates and IT security solutions therefore advises each and every company to follow the three golden rules listed below in their customer communications, so that customers are no longer left to decide for themselves whether shared mail traffic is trustworthy.

The following three steps are essential for protecting customer communications from damaging phishing incidents:

- **Deploy an e-mail signature as basic protection against phishing attacks:**
Companies should digitally sign their e-mails. This precautionary measure doesn't cost much, entails no extra work for senders or recipients and is forge-proof to boot. A signature combined with the attendant certificate lets the customer verify the e-mail sender at a glance, and thus be absolutely secure in knowing whether it is authentic and sent from his or her own bank, insurance company or Internet service provider.

- **Engender trust with open-ended communication:** Companies should inform their customers immediately that in future they will be receiving exclusively signed e-mails and so can safely assume that any unsigned e-mail could not have originated from the purported sender. Customers can adapt their behaviour accordingly in terms of reading their e-mail and thus protect themselves from falling victim to a phishing attack.
- **Allay customer uncertainty with information campaign:** Finally, it's important that companies explain to their customers clearly and specifically what a signed e-mail is and e-mail is and how they can recognise a signed message. A screenshot of a signed e-mail or signature can be useful in this regard. The easier it is for customers to perform the check, the more likely they will be to perceive the security measure as a customer service and to accept any extra effort on their part in exchange for greater security.

“Around 94 per cent of all spoofed mails pretend to be from financial institutions. The rest of them are distributed particularly among ISPs, official agencies and providers of luxury goods. But the creativity of the online counterfeiters is unending,” says Dr. Rolf Lindemann, Director of Product Management at TC TrustCenter. “Accordingly, all companies should set the goal of protecting their customers’ interests and taking effective, coordinated security measures together. That’s the only way businesses can sustainably maintain their customers’ trust in their cooperation, as well as protect their own name from being hijacked and their customers from criminal activities.”

TC TrustCenter offers a range of anti-phishing certificate solutions for companies of every size. Information about the individual solutions and about how companies can deploy e-mail signatures is available at <http://www.trustcenter.de>.

*“APWG Phishing Report“ July 2006; can be downloaded at <http://www.antiphishing.org>