



NEWS BRIEFS

How Companies Can Determine Policies for Instant Messaging

Companies started embracing instant messaging technology for fast communication and productivity increases, but policies governing this medium should set parameters for security, archiving, and other functions. Depending on the firm's industry, security and archiving protocols may be more stringent than for other industries. Executives will want to consult with IT and legal staff about compliance necessities with regard to instant messaging communications. Free consumer IM products are available, but they lack security such as data encryption; some firms could turn to AOL's AIM Pro, which is still free but offers encryption and other security features as well as voice- and video-conferencing. However, even AIM Pro is vulnerable to malware because it sits beyond a system's firewall. For firms interested in IM as a communication, collaboration, and productivity tool with a need for security enhancements, enterprise platforms are best, including platforms from Microsoft, IBM, and Novell. These enterprise solutions sit behind the network firewall and provide virus scanning, encryption, and internal policy enforcement.

Airports to Inspect ID Cards With Black Lights

Security screeners in U.S. airports now use black lights to verify authenticity in passports and other official documents. Transportation Security Administration officials use the small, inexpensive black lights to illuminate holograms on passports and other IDs in order to spot forged or altered documents. Since June of last year, airport authorities have arrested more than 40 individuals attempting to pass through customs with fake documents, and many of those apprehended were charged with violations relating to immigration. TSA officials soon will use an estimated 2,100 lights at the nation's 800 airports checkpoints, while also observing crowds for suspicious activity or behavior.

Vishing Attacks Rise Alarming, Internet Crime Complaint Center Warns

A new wave of security attacks has been reported by the Internet Crime Compliant Center that asks consumers to provide personally identifiable information through mobile phone browsers or by requesting it over the phone. The vishing attacks, otherwise known as voice phishing, send text messages indicating users' bank account information has been tampered with and the user must access their account by clicking on a fraudulent link to resolve the situation. Users are also encountering vishing schemes involving calling a pseudo bank telephone number to clear the alleged security problems regarding their account; an automated "bank" greeting then prompts the user to provide their card numbers. The criminals waging the attacks have attempted to brand themselves as legitimate parties by inserting their own malware warnings and cautioning users about fraudsters. Similar attacks have been reported by the IC3 involving impersonation of FBI officials and agents, employing actual letterhead or images from the federal agency to appear legitimate. The IC3 has warned users to contact their financial institutions using phone numbers from sound sources such as bank statements.

NEWS YOU CAN USE

Ban The Bully

Roughly 54 million U.S. employees suffered from workplace bullying at some point, according to a recent poll by Zogby International and the Workplace Bullying Institute. In response, supporters of "Healthy Workplace" projects submitted legislation in 13 U.S. states to protect and support intimidated workers. These laws would resemble federal and state anti-discrimination laws, providing protection to all employees regardless of race, age, or gender; but victims would have to prove their health had been harmed by the incidents in question. Moreover, employees would have the option to accept workers' compensation benefits in lieu of filing suit against their employers, according to the proposed legislation. One former emergency-room secretary is pushing for the legislation in Vermont after she lost her job at a local hospital after complaining to the hospital board about a nurse manager and other supervisors' bully-like behavior. She says hospitals that allow bullying to take place are not only placing workers in danger, but patients as well. Experts, on the other hand, are urging human resources (HR) departments to devise their own anti-bullying policies to stave off workplace skirmishes and future litigation. Victims of workplace bullies often cite subsequent health problems, including depression. In one case pending in Indiana's court system, an employee is suing his former hospital employer for over \$325,000 in damages after being bullied by a heart surgeon. According to the Workplace Bullying Institute, bullying can go beyond verbal threats and involve work interference and humiliation.

ALERTS



Security Condition SecCon 3



[Click Here for More Information](#)



If you have any feedback, or if you feel that you have received this in error, please e-mail michaeltaylor@chesleybrown.com or call (770) 436-3097