

An e-Valentine's Day massacre

Forget their loving intentions: sending and receiving e-cards could have serious consequences for any unprepared company, warns **Yuval Ben-Itzhak**

» In 2005, an estimated five million e-cards were sent and received on Valentine's Day, many to and from work email addresses. Even more romantically, these e-cards could be sent anonymously. I doubt there are many better and easier methods of encouraging people to actively download dubious programs behind the corporate firewall, which may include some spyware or a virus.

Although most corporations have email and internet policies that discourage using them for non-work related activities, most are resigned to the fact that email and the internet are used for personal reasons during work.

As the use of e-cards increases, so too has the threat from viruses, spyware, and phishing. Just the receipt of an e-card can be a huge threat. Even if it is not opened, the power of love can conquer even firewalls.

Those lucky enough to receive an e-card are likely to be caught up in a cycle of pop-up windows offering romantic breaks or similar offers. Some people ignore these, but for others, curiosity draws them to click on an advert: unknowingly, they have just left the entire company exposed to web-borne security threats.



The power of love can conquer even firewalls.

Yuval Ben-Itzhak, Finjan

Attacks enabled by Active Content, such as executable content, ActiveX control and JavaScripts, are growing and account for the vast majority of today's malware. Sophisticated, content-driven malware applications such as spyware, do not leave 'fingerprints' that are sufficient to identify them.

The use of Active Content technologies presents a security challenge. Active Content is used for regular business practices such as CRM, web conferencing, e-commerce and webmail, which means that it is not productive to simply block all Active Content. Moreover, traditional security solutions, such as anti-virus and intrusion detection systems, are reactive in nature and powerless against unknown and complex attacks.

Instead of relying on reactive virus database updates, companies should look at proactive behaviour-based security solutions that block malicious and inappropriate content before it strikes. Deployed at the gateway, behaviour-based security protects businesses in real time, preventing attacks from reaching local computers.

So, hopefully you didn't get caught out this Valentine's Day. But if you do not protect yourselves with a tighter ring of security, you may leave yourself vulnerable to heartbreak.

Yuval Ben-Itzhak is chief technical officer at Finjan.