



# Protect your family and friends from seasonal online threats



## 500 million e-cards will be sent this Christmas, some of them could contain unwanted 'presents'

**People are turning to e-cards as a low cost and eco-friendly way to deliver the season's greetings to friends and loved ones.**

Yet new research by global internet security firm AVG Technologies found that almost three quarters (74 per cent) of the people it polled said they would automatically open an e-card if it were from a friend or colleague.

It is vitally important that you pick the e-cards you read very carefully.

Criminals are using this growing medium to deliver viruses and other security threats to the computers of their unsuspecting victims. Because risky e-cards are typically made to look like they have been sent from a trusted party, usually a friend or relative, they fool the recipient into opening them.

E-cards are considered such a risk that in America the FBI has issued formal warnings, after fraudulent e-mails were sent in the name of the Deputy Director.

Research from AVG's labs indicates an estimated 500 million e-cards and greetings will be sent online this Christmas.

If only 0.1% of e-greetings sent during this festive period contain a security threat – that's still tens of thousands of damaged or compromised PCs. This many damaged PCs adds up to a great deal in terms of lost family photos and videos, lost work, and emails. Plus compromised PCs often become distributors of spam or their owners may become the targets of identity theft.

The good news is that these internet security threats can be avoided. Experts at AVG Technologies have compiled five tips so that internet users can send and receive e-cards with peace of mind.



## Using e-cards safely

- 1) Don't open attachments: Most legitimate e-cards are links to the company's website that allow you to go directly to your card. Avoid attachments and don't download anything from a source you don't recognise.
- 2) When in doubt, delete: If something looks a little strange or "phishy," such as the name of the sender or vague subject lines, just delete the card. It's better to do that than run the risk of getting a virus or some other form of malware.
- 3) Know where you're going online: Use security software\* that detects and blocks web sites that push online scams, adware installations, attachments filled with viruses and other malicious downloads that could harm your system.
- 4) Know what to look for: While most e-card scams actually look legitimate, there are usually some tell-tale signs to look for. Watch out for misspelled words or names, not knowing who sent you the card, a disguised name (such as Your Friend, A Secret Admirer, etc.), and a strange web site address.
- 5) Always read fine print before accepting any terms: Make sure you actually read the fine print before agreeing to anything. Some e-card scams list in their terms that they can send email to everyone in your address book. Make sure you know what you are agreeing to.



*\*This doesn't have to cost a cent: download AVG Anti-Virus Free Edition 8.0 with LinkScanner technology here: [www.avgfree.com.au](http://www.avgfree.com.au)*

## Internet Security — What does AVG recommend?

**Essential protection:** Parents should ensure the home computers have anti-virus, anti-spyware and firewall protection, at a bare minimum. A product such as **AVG Anti-Virus plus Firewall 8.0** is a good, affordable solution. This will enable you to block malware and peer-to-peer nets with illegal content.

**Safe search and surf protection:** The LinkScanner safe search and safe surf protection built in to all AVG commercial products provides the best protection available from online threats. Web pages known to be bad are highlighted when you search so that you know not to visit them. Plus the web pages of all links you click as you browse the web outside of search engines are quickly scanned for threats in real-time, before you actually visit them.

**Spam protection:** "Spam" is the term used to describe junk e-mail (which often includes unpleasant content and malicious malware in attached files). Because spam e-mail and attached malware has increased to such intrusive levels, you need to protect your family from spam. The **AVG Internet Security 8.0** full suite solution provides comprehensive protection against all online threats, including spam e-mail.

**Backup protection:** Data loss is an important topic that nobody worries about until it happens to them. A backup of the documents, photos and other files that you can't easily reproduce is important. Ideally the second copy is kept physically separate to also protect against fire, flood or theft. **Carbonite Online PC Backup** is a very cost effective, set and forget solution.

**Update, update, update:** It is especially important to keep the operating system software that runs the computer, security software that protects your computer and software you use to access the Internet, up-to-date. Indeed, the more regularly all of your software is updated, the safer you are. It is ideal to have your software set to update automatically. Any software that is not up-to-date is potentially vulnerable.

There are no radical technology solutions, so using parental controls and being aware of what your children are doing online is the first line of defence for children. Awareness of the problem is the first step to a solution.



Tough on threats. Easy on you.  
**avg.com.au**