Small Business Security Guides

How to let staff use their Personal Technology Securely

AVG | AT WORK

How to let staff use their Personal Technology Securely

More and more of us would like to use our personal computer at work, but how can companies allow that while keeping their internal networks secure?

Did You Know?

- End users, not the IT department, will be responsible for 50 percent of business IT procurement in 2010
- Virtualisation specialist Citrix has a "Bring Your Own Computer" program which saves the company money
- One-third of the new generation of workers want to choose their hardware and applications

Why Traditional Anti-Malware Solutions Are No Longer Enough

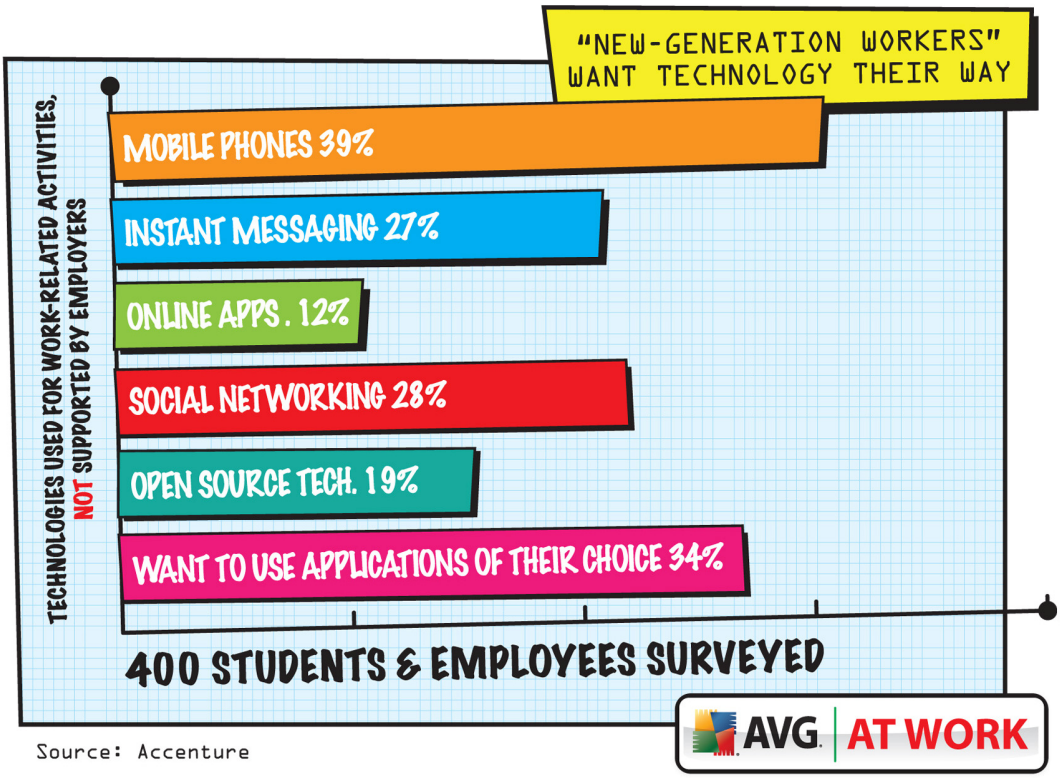
Given the P in PC stands for 'Personal', it's not surprising that many consumers have a close relationship with their computer in a way that isn't traditionally associated with other appliances. Very few heated conversations over coffee, centre around one brand of one washing machine being cooler than another. Conversely, put a Mac and PC fan in close proximity, and things will eventually get ugly.

This emotional bond to personal technology - which also extends to mobile phones, MP3 players and notebook computers - means businesses have increasingly had to adjust to requests from staff to use their own technology at work. Few companies insist on staff wearing clothes provided by the company to work, and as technology shifts from the merely functional to the fashionable, some employees expect the same level of personalisation to be permissible.

According to research by technology analyst group Gartner, by 2010, end users, not the IT department, will be responsible for 50 percent of business IT procurement decisions. It is becoming increasingly unlikely that a department head or IT manager will decide what PC or mobile phone employees should use. Other recent research by management consultants Accenture, focused on a group of young workers it calls "Millennials", their research revealed that around one-third of this new generation of workers not only wanted to use the computer of their choice at work, but also wanted control of the applications they use too.

"The message from Millennials is clear: to lure them into the workplace prospective employers must provide state-of-the-art technologies," said Gary Curtis, managing director of Accenture Technology Consulting. "And if their employers don't support their preferred technologies, Millennials will acquire and use them anyway."

Businesses are reacting to the trend towards personal technology at work in a variety of ways. For the more traditional firms, the idea of giving staff carte blanche to bring their own technology to work is totally unacceptable. Allowing an employee to bring her sticker-festooned game-spec laptop to work is tantamount to a written invitation to stop working and indulge in personal surfing during business hours. More progressive companies realise that allowing personal computers in the office is just another step in the blurring lines between work and home.



However, while some companies might want to reduce the restrictions on consumer technology at work, there are impediments to engendering an atmosphere of indulgence that goes beyond cultural concerns - namely IT security. The requirement to standardise technology across a company has some financial benefits in terms of volume buying, but studies by some companies have shown that giving staff a stipend to buy their own device and effectively support it, can result in a lower cost than realizing the savings from large scale procurement and paying IT support staff to maintain the devices.

Instead of focusing on saving cash, some companies insist on a homogeneous approach to PC procurement across the business as it is perceived to be the easiest way to ensure that PCs and mobile phones can be secured effectively. The more standard the hardware, the more easily it can be monitored, patched and updated centrally. The emergence of so-called virtualisation technology however, offers a potential solution to the problem of allowing staff to use their own technology without compromising the security of the company's network and data. Virtualisation has become very popular in computing circles lately but actually dates back decades to the days of large centralised computers called mainframes. Mainframes used virtualisation to effectively slice up the machine's power so multiple tasks could be carried out simultaneously without disrupting each other. This approach is now applied to modern day servers and even personal computers to sever the link between the computer's operating system and hardware. Traditionally, desktop computers have only been capable of running one operating system at a time, but with virtualisation, they can run multiple instances (virtual machines) of the operating system to be run on the same piece of hardware.

Analysts like Gartner, advise companies to use this virtual machine approach to effectively create a safe compartment within an employees' personal computer, or even mobile phone, so that any interaction with the company's network is limited to that safe-zone. Instead of loading company applications onto their home machine - and creating licensing issues - staff can access a secure and virtualised set of applications held on the company's servers. This also prevents users from infecting the company network with any malware that might be on their machine, and from copying and storing sensitive data outside the firewall. Gartner believes that there are other strong motivations for organizations to consider employee-owned notebook programs based on a locked and well-managed VM approach: "They provide a mechanism for 'containing' the operational environment of existing rogue users. This category usually consists of executives and key knowledge workers, whose personal influence is sufficient to be able to flout corporate policy (with exceptions permitted on the basis of trust)."

Businesses that are already using a virtualised approach to managing employee-owned devices include Citrix, which launched a "Bring Your Own Computer" program in 2007. This plan makes use of the company's own virtualisation technology to allow staff to use their own hardware at work. Employees install software called the Citrix Receiver onto their computer, and are then able to access corporate applications and data securely.

The increasing adoption of virtualisation for desktop machines means that more and more companies may be able to cut the ties between hardware and software and allow users to bring their own technology to work. However, as technology becomes more prevalent, it unfortunately becomes a greater target for hackers and cybercriminals. As you can imagine, the personal connection between computers and their users is unlikely to diminish anytime soon, so as the bad guys find the chinks on the virtualisation approach, the security community will strive to evolve fresh ways to protect the devices we need and love.


AVG SMB group at:
bit.ly/avglinkedin


Become an AVG Fan at:
facebook.com/avgfree


Read our blogs at:
blogs.avg.com


Follow us at:
twitter.com/
officialAVGnews


Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com