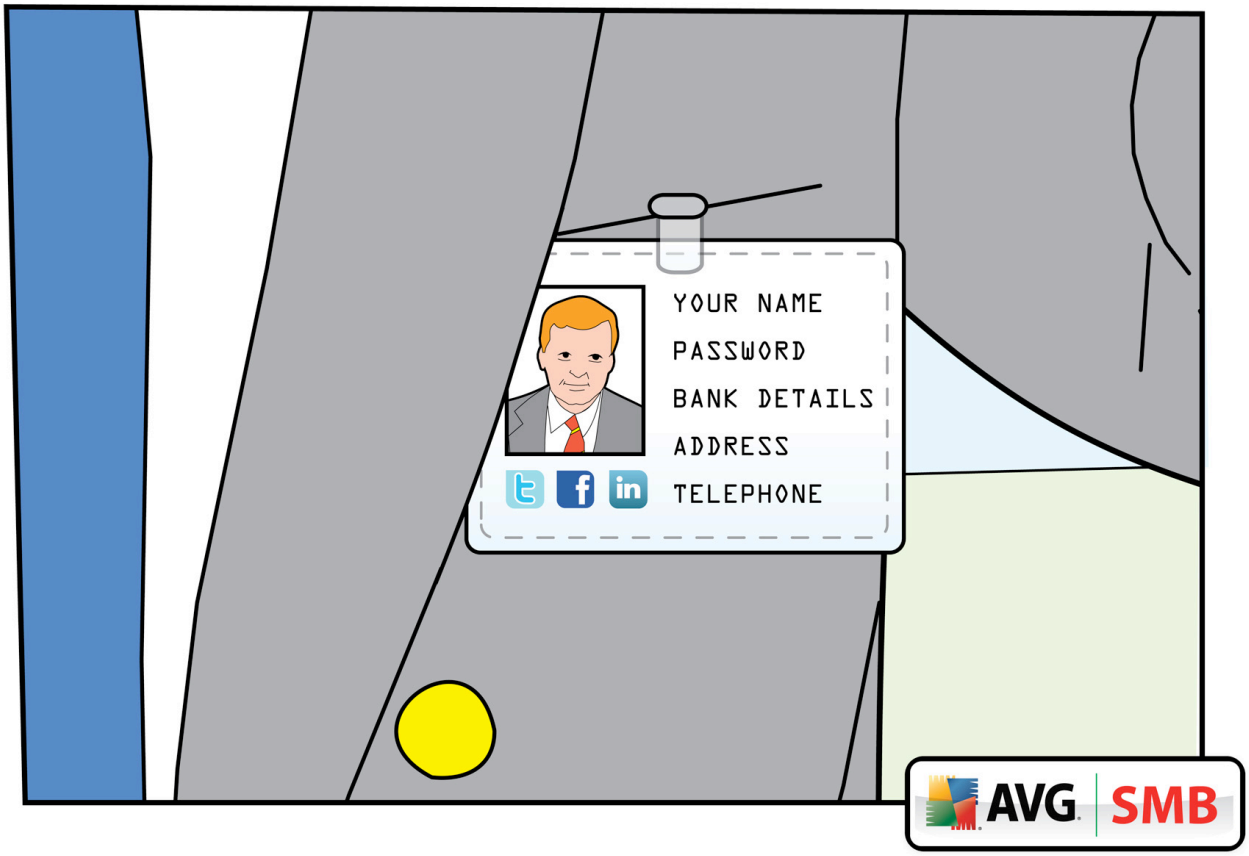
Small Business Security Guides

Top Tips to Securing your Business Reputation

AVG | AT WORK

Top Tips to Securing your Business Reputation

I've been reading with interested the recent reports of how a Twitter scam has affected some well known politicians, issuing embarrassing Tweets from their personal accounts. Whilst these headlines may seem amusing, it is worth considering the potential impact of this type of scam on your business reputation. Reputation is everything in the world of a small business, often taking years to establish. Being targeted by a similar scam can have a detrimental effect on the reputation of your company. In a recent NCSA (National Cyber Security Alliance) study on small business security, 69% of small business owners said they would let their customers know if they suffered a security breach, whilst almost half agreed that their customers are concerned about the IT security of their business.



Knowing that a supplier's IT infrastructure is not as secure as it should be would worry most people, particularly if they share critical business data with that supplier/company. Yet with so many more businesses using cost-effective social media tools to market their company, the threat of customers being sent inappropriate messages from your (or one of your employees) social media account is real and the potential impact on your reputation (by undermining your customer's trust in your ability to safeguard their data) is great.

So to help safeguard your business reputation, here are a few tips to ensure you get the most out of your security software, allowing you to focus on building your reputation, not repairing it:

1. Make sure your security software is robust and up to the job. AVG software is certified by the major independent security certification bodies to be effective against a comprehensive range of threats.

2. Secure your network against insecure behavior by employees. You can't always control where your staff goes online at work (if you do, you'll probably have a rebellion on your hands). AVG's Business Edition contains LinkScanner® which stops users visiting

poisoned websites that can let hackers into your network. So make sure it is installed on every PC.

3. Set your security software to update itself at least once a day. Protect against new and unknown viruses that appear between updates by ensuring AVG Data Protection is active on all workstations. AVG's Business Edition Internet Security contains the Data Protection module.

4. Make sure you set the highest level of security on laptops employees take home or on the road. Once those PCs are disconnected from the network, they're out of your control, so leverage the power of AVG's internet update packages to keep their protection solid.

5. Deal with computer security problems as soon as they arise. AVG optionally alerts you whenever it finds a problem – day or night – and takes the necessary action to protect your network automatically – you don't have to do a thing. If you have the time, review the log – it can give you valuable information about employee training or other preventive measures that will help improve security.

Has your business reputation suffered from an online scam? What actions did you take to prevent a repeat?


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