# While You Are Away For Christmas, Who Has Access To Your Network and Data?

Submitted by: GFI Software
Tuesday, 18 December 2012

---

GFI Software warns that IT security complacency and lax access and device policies over the Christmas and New Year shutdown are ripe for exploitation by cyber criminals

London, UK – 18 December 2012 – GFI Software™ today released guidelines for businesses ahead of the Christmas and New Year holiday period, traditionally a time when many office-based businesses close for the festive season, leaving IT departments unmanned and key IT systems at heightened risk of hacking and denial of service attacks, malware infections and unauthorised access.

This year brings the added challenge of end-user devices being used to remotely access company resources, in particular email, following a surge in sales of iOS®, Android™ and Windows® 8-based tablets and smartphones. An unprecedented number of users will remotely access company resources for the first time – with varying levels of knowledge and care – using devices with varying levels of security in place to protect the user, the data and the connection into the network.

“The Christmas holiday season traditionally poses a big challenge for organisations of all sizes, as the need to monitor and maintain IT systems has to be balanced against the need for staff to take time off,” said Phil Bousfield, GM Infrastructure, at GFI Software. “However, IT staff face additional challenges, as not only do they need to consider the reoccurring threat of networks and systems being targeted during the quiet holiday period, but also the risk posed by employee devices being used for remote access.”

The “bring your own device” (BYOD) culture within many organisations is set for massive uptake following record sales of tablets and smartphones this Christmas. Global tablet shipments in 2012 are set to reach 87.7 million units, according to analyst firm IDC, while RBC Capital predicts that 30 million iPad® and iPad Mini® units alone will be sold in the run up to Christmas – double the number sold in the run up to Christmas last year.

“This wave of new devices will undoubtedly bring with it a surge in users accessing corporate IT resources from non-company equipment, with varying levels of security in place. What might seem like a useful productivity device can in fact be a security flaw and a route into your network just waiting to be exploited,” added Bousfield.

Combined with the added risk of external network intrusion, malware infections and natural disasters, such as power cuts, burst pipes and burglary, the risks are higher than ever if not adequately addressed ahead of time.

GFI Software recommends the following precautions to ensure that networks and servers are as robust as possible in the face of heightened security threats over the holiday period:

• Remove redundant user accounts: It is imperative that system and application user accounts belonging to former employees, or belonging to current employees no longer needing them, are purged. Dormant user

accounts – known as Ghost Accounts – pose one of the biggest risks of unauthorised access and increase the number of entry points for an opportunistic hacker.

• Shut down unnecessary open ports: Check routers and gateway appliances to make sure that only the most critical network ports are open. Closing unused ports greatly reduces the risk of intrusion, as well as helping to interfere with malware, spyware and other malicious code trying to communicate under the radar of port monitoring software.

• Patch all software: Before shutting down for the break, make sure that all operating system and key application patches have been applied. A dedicated patch management (http://www.gfi.com/network-security-vulnerability-scanner/patch-management) solution will automate the process of both finding and deploying patches to all machines on the network, reducing the workload of IT staff throughout the year as well as the risk of operating system and application vulnerabilities being exploited.

• Update antivirus software: Ensure that both the antivirus application (http://www.gfi.com/business-antivirus-software) and the definition files on all servers and other critical equipment are up-to-date. While systems are being left unattended, it is imperative that malware defences are as robust as possible to prevent accidental or intended infection of key systems, such as mail servers.

• If you don’t need it – switch it off: Non-essential systems should be shut down while the business is closed. This will reduce the risk of unnoticed equipment failure and prevent non-critical systems from being compromised and used to access critical systems and storage silos.

• Refresh the IT policy: If your organisation doesn't already have a policy regarding BYOD – set one. The same applies regarding the required security levels of any device used to connect to company resources either remotely or within the building. An unsecured tablet is a potential threat to data security and compliance.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organisations on a global scale. The company has offices in the United States, United Kingdom, Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold ISV Partner.

For more information:

GFI Software

Please email David Kelleher at dkelleher@gfi.com
GFI - Malta: Tel: +356 2205 2000; Fax: +356 21382419.
URL: http://www.gfi.com.

Davies Murphy Group
Please email Chris Green at gfi@daviesmurphy.com
Tel: +44 1256 807360