

Information security threats in the home and the office are very similar, with the possible exception of targeted attacks. However, the controls which we take for granted in the office environment, such as multi-layered anti-virus, hardware firewalls and content management may be absent at home. Whilst technical infosec professionals are likely to have better security than the average person, they may still mix work and personal activities on the same network or even the same computer. Unless proper segregation of networks is employed, preferably with separate Internet connections, there is a very real risk of exploitation by an attacker or accidental exposure of information.

Most people's mindsets will be different and often more vulnerable at home, even if they are infosec professionals. Our guard may be down and we may feel it unnecessary to lock our workstations or monitor our blogs and social networking activities as closely as we do at work. Yet this relaxing of the boundaries is precisely what leads to the inadvertent release of sensitive information. Family members may be permitted access to a network which is also used for work-related activities and are unlikely to be subject to proper controls or monitoring. Younger family members may attempt to share files and open ports to peer to peer networks, exposing the home environment to external abuse. Home networks may contain games machines which undermine an otherwise secure network, by requiring weaker wireless encryption or introducing protocols such as Universal Plug and Play which can lead to router hijacking.

Infosec professionals are more likely to understand the real risks of, for example, web browsing and implement tools such as NoScript to protect themselves. However, their family may not be so aware and simply "click through" the warnings from protective tools without understanding the consequences. Most people still operate with full administrative privilege on home systems, leaving even the best defended machine open to accidental compromise. Of course, enthusiastic infosec professionals may be tempted to employ "belt and braces" security, resulting in controls which other family members find obstructive, resulting in attempts to bypass security and exposing them to attack.

The majority of employers still expect home workers to use their domestic networks for remote access, even when they provide a company laptop. Few provide proper guidance or clear standards for configuring home networks and rely on the configuration of the laptop and VPN to provide security. Yet inadequately secured home wireless networks provide the perfect opportunity for a targeted attack against these laptops and hence the corporate network. Ideally, organisations should provide dedicated connections for remote workers, but most consider the cost of implementing and maintaining such connections too high.

Peter Wood is CEO at First Base Technologies, an ethical hacking firm based in the UK, and a member of the ISACA conference committee. Peter founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as social engineering, network penetration testing and skills transfer. Peter is also a world-renowned speaker and security evangelist.

Peter Wood
peterw@firstbase.co.uk
www.firstbase.co.uk
www.white-hats.co.uk
www.peterwood.com