

BYOD* security is no LOL matter

* Bring Your Own Device



81%

...use a personal electronic device for work-related functions.



31%

...who use a laptop for work will connect to the company's network via a free or public Wi-Fi connection.



46%

...who use a personal device for work have let someone else use it.

Tip: Provide cybersecurity training to all BYOD employees that includes physical security, WiFi security and social engineering attacks. Include at least four hours of face-to-face learning.



37%

...who use personal device(s) for work have not activated the auto-lock feature.

Tip: Make password-protected auto-locking a requirement on personal devices used for work. Make sure employees know what makes a password strong.



33%

...who use their personal device for work admit that their organization's data and/or files are not encrypted.



66%

...who use a personal device for work say their organization has not implemented a "bring-your-own-device (BYOD) policy."

Tip: Develop and enforce a clear, written policy that lets employees know what work-related data they may access with their own devices.



25%

...of employed U.S. adults have been a victim of malware or hacking on a personal electronic device.



Internet Security

www.eset.com