Advice On Bringing Your Own Device To Work

(NAPSA)—When employees can have all their personal and work information at their fingertips, it can be a big help—and a major headache—to them and their employers.

The Trend

Increasingly, workers today are bringing their personal devices to the company IT department to enable access to e-mail and other productivity apps on them.

According to a recent Forrester report, three-quarters of U.S. workers pick the smartphone they want rather than accept IT's choice. What's more, another recent survey discovered increasing numbers of enterprises across all industries are supporting a bring-your-own-device (BYOD) model, and in more than half of those instances, employees shoulder the cost of their device and service plan.

The Problem

So now employees can use their favorite devices for work but companies must support more platforms and deliver business apps including e-mail, chat and portals on iPads, iPhones, Android and Windows phones. That means that data and apps will be used from any location over any network—which can endanger sensitive company information, potentially getting workers or their employers into trouble.

To keep confidential data stored on personal mobile devices from falling into the wrong hands, many IT departments turn to third-party solutions to better secure, monitor, manage and support the variety of mobile devices used by employees. Using one of these solutions, IT organizations can implement security controls such as passwords and remote wipe and lock, which lets IT erase corporate data from a mobile device in the event it's lost or stolen.

If Santa brought you a new smartphone or tablet, here are some tips from Good Technology to keep your device and information safe.

The challenge is that most employees don't want to enter a complex password every time they need to make a phone call, send a text message or update their Facebook status. Plus, when employees use their personal phones for work, a remote wipe could erase personal apps and data in addition to corporate data and applications.

A Solution

Fortunately, companies such as Good Technology take a different approach to these BYOD security challenges and keep the best interests of employees and the company in mind. Good helps companies separate and secure corporate data while leaving employees' private information untouched.

For example, rather than remotely wiping the entire device, IT can wipe only corporate data, leaving personal data and applications intact. This lets employees use their personal mobile devices at work without having to worry about compromising company information.

Keeping Information Secure

1. Don't use cloud programs on your mobile device to share corporate files and data.
2. Beware of e-mail fraud. Don't send e-mail to anyone you don't know or respond to e-mails from unknown sources without first verifying that they are legitimate.
3. Secure your device's settings and have it automatically lock after five minutes.
4. Don't forward e-mails from your corporate address to private e-mail accounts, especially e-mails with attachments.
5. Don't use check-in apps everywhere.
6. Turn location setting off when not using apps that require it.
7. Be careful of beta programs/apps—they can be dangerous, as in many cases the developers haven't sorted out security yet.

Further Information

To learn more, visit www.good.com or call (866) 7-BE-GOOD.