blancco

5 Important Data Privacy Tips Your Employees Must Know

Data Privacy Day (known as Data Protection Day in Europe) is an international holiday that occurs on January 28th every year to raise awareness about data privacy and promote data protection best practices. With new data breaches emerging daily, it's important for organizations to provide employees with actionable data protection tips and recommendations.

Talk to your employees today to help them understand when, where and how their data could be compromised – and how to prevent that from happening. Share these tips and celebrate Data Privacy Day at your organization.

Tip 1: Just because you can't see files on your desktop/laptop computer doesn't mean they're gone.

When you drag files to the Recycle Bin on your computer and/or reformat your hard drive, the data isn't really gone. Imagine your hard drive is like a library. To find the book you want, you get a reference number from the library's database – and that leads you to the section of the library where the book can be physically found. Deleting the file is like deleting that reference number. But the book still remains in the library, and it just becomes a case of using more sophisticated methods to locate it. Secure erasure of your files is the best way to make sure your data is truly destroyed.

Tip 2: Beware of what you're syncing.

How often do you charge your personal smartphone by plugging a USB cord into your company laptop? How often do you charge your work phone by plugging a USB cord into your personal laptop? Chances are, you take these actions multiple times a day. Once connected, a lot of devices begin automatically syncing without notice and transferring files between the two. If you're plugging devices into one another, beware of which files you may be transferring and whether sensitive information like photos, emails, contacts and usernames and passwords could be hacked and eventually leaked.

Tip 3: Formatting removable media (i.e. SD cards, USB sticks) isn't the same as erasing data.

External SD cards make it easy and efficient to transfer data from device to another, but they also increase the chances of sensitive information being leaked. Why? Emails, contacts, photos, videos and other files can be saved on the SD card instead of the device itself. If the SD card is lost or stolen, data can be easily transferred to another device. And formatting removable flash media, such as USB sticks and SD cards, doesn't actually erase the data forever. If not properly deleted, all of those photos, videos and other sensitive files could very well come back to haunt you. To securely erase an external SD card so that the data can never resurface, you first have to remove the SD card and insert it into a computer. This can correctly detect all of its sectors and run software to securely erase everything.

Tip 4: If your smartphone is undergoing repairs, don't forget to erase data from a loaner device.

Are you experiencing issues with your mobile device? Have you taken your device into the retail store of your carrier or device manufacturer to have it tested and repaired? If this happens, you might be given a temporary "loaner phone" to use until your own phone is fixed, which could take about one week or possibly longer.

In the meantime, you've probably been using the loaner phone to save new contacts, photos and videos, as well as send emails from your work email account. But when it's time to get your own phone back and return the loaner device, make sure all of that data has been permanently erased. And remember, if you have an Android device, a factory reset doesn't properly erase the data; it leaves exposed and potentially accessible to the next person who uses the loaner device.

Tip 5: When you close an account with a business or website, ask for proof.

When the personal information of over 32 million registered users of dating website Ashley Madison were leaked, the consequences were profound. Even though users paid for the site's $20 "Full Delete" program, the understanding was that their information would be removed completely from the site. But that didn't actually happen and users had their data resurface. The lesson here? Always ask for proof that your data has been permanently erased from all locations where it's being stored.

DATA PRIVACY IS A SERIOUS ISSUE. KNOW THE FACTS.