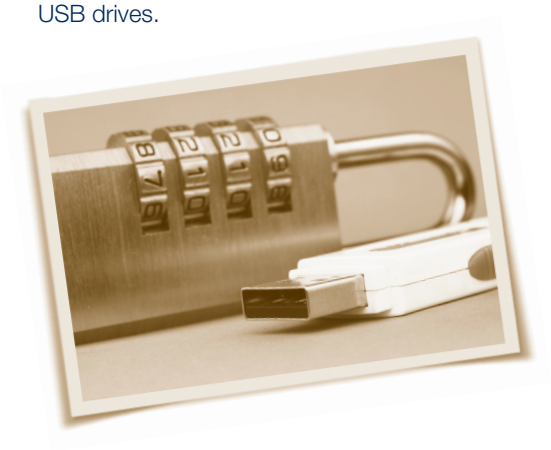
Security Awareness Tips

USB Flash Drive Security Best Practices

USB flash drives, or memory sticks, are data storage devices for your computer that are typically removable and rewritable. The small size of the device makes it highly portable – but also creates a concern for data security. A recent study by the Ponemon Institute revealed that while these devices may be small, the data breaches that can result from lost or stolen USBs are huge. Organizations and employees need to properly manage the security and privacy requirements of data retained on USB drives.



What Can Organizations Do?

- Provide only approved, quality USB drives for use in the workplace. To help mitigate the risk of loss of confidential data being placed on the USB drive by employees, invest in encryption software for the drives prior to handing them out.
- Be aware of how your organization's computers work. Some can be set up to be bootable from a USB drive. Tech savvy thieves could use a flash drive containing a portable booting operating system to access the files off a computer even if the computer is password protected.
- If your organization is still unsure about the use of USB drives, some computers can be configured to disable their use. USB ports can also be disconnected within the computer before employee use.
- Develop a policy about appropriate and acceptable use of USB drives including what data may be stored on them and where they should be kept when not in use.

Employee USB Safety

› Tether your USB device to a lanyard or keychain so it can easily be found.

› Lock or password protect your USB device.

› Do not store sensitive information on the drive.

› Most USB drives will allow users to divide up their file capacity into a public area that can be used by anyone who has the drive and a protected private area that requires a password or even fingerprint. Carefully select the correct areas when saving.

› Keep your personal information and work information on separate USB drives.

USB flash drives can be used safely and securely if the risks are understood and proper measures are taken to mitigate them. Company security policies should always be followed.

For more information on USB drive security...

The State of USB Drive Insecurity:
http://www.itbusinessedge.com/slideshows/show.aspx?c=91980

New Security Risks from USB Flash Drives:
www.earthlinksecurity.com/articles/usbdrives/index.html

AlliedBarton® Security Services

Local Response | National Support