

CYBERSECURITY TIPS: USING CAUTION WITH USB DRIVES



What security risks are associated with USB drives?

USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and portable, so they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

- Attackers can use USB drives to infect other computers with malware when the USB drive is plugged into a computer.
- Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production.
- Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive.
- Even computers that have been turned off may be vulnerable because a computer's memory is still active for several minutes without power.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

The full article can be found at us-cert.cisa.gov/ncas/tips/ST08-001

Article provided by **Cybersecurity & Infrastructure Security Agency**.

Please visit us-cert.cisa.gov/ncas/tips for more information.

First Bank Chicago



Your Interest Is Our Priority

HIGHLAND PARK
Banking Center
(847) 432-7800

NORTHBROOK
Banking Center
(847) 272-1300

SKOKIE
Banking Center
(847) 272-7800

WESTCHESTER
Loan Production Office
(708) 223-7001