MALWARE EVERYWHERE: YOUR COMPUTER IS UNDER ATTACK p. 86

CURING THE DISEASE BEHIND ZOMBIES & WEREWOLVES p. 106

WIRED

Do you *really* want to be like Steve Jobs?

He was a **Buddhist**...

... and a **tyrant**.

He was a **genius**...

... and a **jerk**.

How his life story has become an **inspiration** *for some ...*

... and a **cautionary tale** *for others.*

0 75110 08459 2 08>

$4.99 US | FOR

Portable Secure Hard Drives

No matter what you're protecting—bank records, photos from Vegas—nothing will guard it better than a hardware-encrypted data safe. —Michael S. Lasky

Pocket rocket

EDITOR'S PICK

Apricorn Aegis Padlock 3

8 RATING

The Aegis Padlock is fast and brawny—its USB 3.0 data transfers are nearly 10 times quicker than USB 2.0, and the built-in AES encryption chip (choose between 128- and 256-bit protection) is coated in epoxy, which can't be compromised without damaging the circuitry beyond repair. Though muscular, the 6.2-ounce Padlock is small enough to slip into your pocket, and it comes with an integrated USB cable you'll never lose. Usability is an issue, though: While the initial setup was easy and the keypad registers strokes accurately, creating individual passcodes for multiple users was frustrating and required too much manual-digging.

WIRED **Warp-speed USB 3.0 file transfers. Good for groups: Stores up to 5 unique passcodes. Configurable auto-lock has a self-destruct feature that wipes the drive when intruders try to get in.** TIRED **Confounding passcode management. Hogs two USB ports on some computers.** $190 (500 GB)

THE BASICS

What extra protection does hardware encryption add?

A system password is a software program like any other, so a determined thief can remove the hard drive from your computer, mount it on another machine, and crack the password. But these drives won't even mount on a PC desktop unless you first pass a hardware-based authentication test: typing a PIN on a keypad, swiping a fingerprint, tapping an RFID badge, or entering a code displayed on a separate dongle. Fail the hardware tests and the drive locks up. Even if somebody cracks open the case and removes the drive, there's still a 128- or 256-bit military-grade encryption algorithm built into the firmware, so your data is run through a digital Cuisinart before it's even written to the disk, rendering it unreadable.

So they're uncrackable?

No. No encryption is. But if you store your sensitive info on one of these drives, there's a very good chance nobody will ever see it without your say-so. Brazilian and FBI codebreakers spent two years trying to decipher data on the hardware-secured drives of a Brazilian banker suspected of money laundering—before giving up in 2010.

What if I lose my passcode?

All these drives have an admin mode; admins can create codes for up to 10 or so users and can reset a forgotten code. If you're not the admin, the "forgot my passcode" drill is somewhat forgiving. You get up to 25 attempts, after which the drive will require a factory-programmed fail-safe code to enable more PIN entries. After 50 or so failed attempts, the drive assumes it's under attack and self-destructs.

BUYING ADVICE

These drives cost two to five times as much as unprotected drives—if you just want to stash your Beatles MP3s, look elsewhere. Chip-based 256-bit encryption and security features like automatic self-destruct are the norm, so all these drives offer the same base level of protection. Your decision should come down to transfer speed, keypad usability, and, if your data is top-secret, the inclusion of secondary authenticators like smartcards and RFID readers.

Shape-shifting keypad

DataLocker DL3 With RFID

7 RATING

Typing on the DL3's backlit touchscreen keypad is easy, but you're also protected against "shoulder surfers" by a randomizer that shuffles the key layout after each use. What appears to be a normal keypad with sequential numbers one time will have a totally different order the next. Our DL3 came with an RFID module for secondary authentication, which requires you to tap a small RFID card against the drive to gain access. Sadly, the DL3 lacks a time-based auto-lock, so it's suitable as a stash box only for the true paranoid who would never leave it attached and unattended.

WIRED **Layered security: RFID, PIN, keypad scrambler, and AES 256-bit encryption. Best touchscreen we tried.** TIRED **No auto-lock = security hole. Supports USB 3.0, though read/write speeds are not its strong suit.** $430 (500 GB)

Rocstor Rocsafe MX

5 RATING

To access the Rocsafe, you need to enter a PIN and insert a smartcard. Add the 256-bit AES encryption chip and you've got a system so tight even the CIA can't gain entry. Too bad there's no USB 3.0 speed. We'd also like to see an auto-lock feature that would shut the drive off after a set period of inactivity. Another quibble: The touchscreen keypad offers a way-too-brief visual cue that a key touch was accepted, leading us to mistype our PIN too often.

WIRED **Strong multilevel security. Rugged case can take a beating. Includes two smartcards.** TIRED **Only USB 2.0 and FireWire ports. No auto-lock. Very expensive.** $589 (750 GB)

Lenovo ThinkPad USB 3.0 Secure Drive

8 RATING

Lenovo's secure hard drive is wrapped in the same velvety black skin found on the company's ThinkPad notebooks, and it has the same excellent key-feel, too, so we never mistyped a PIN. It's great for businesses or small workgroups—admins can set up to 10 unique user passwords, making secure sharing easy. It also travels well; the pocket-size slab weighs just 7 ounces, and a 16-point omnidirectional shock-mount system guards against accidental drops. It's reasonably fast, too, though not up to the Apricorn's blazing pace.

WIRED **Alphanumeric keypad was the best we used. USB cable is attached—no pieces to forget.** TIRED **Could be faster over USB 3.0, and transfers over USB 2.0 are glacial. Maximum available capacity is only 750 GB.** $170 (500 GB)

PHOTOGRAPHS BY **GREG BROOM**