New USB cable kills your Linux laptop if stolen in a public place

Building your own BusKill cable costs between $20 and $45.

💬   in   📑   f   🐦   ✉️

By [Catalin Cimpanu](#) for [Zero Day](#) | January 2, 2020 -- 21:56 GMT (05:56 SGT) | Topic: [Security](#)

A software engineer has designed a so-called USB "kill cable" that works as a dead man's switch to shut down or wipe a Linux laptop when the device is stolen off your table or from your lap in public spaces like parks, malls, and internet cafes.

The cable, named **BusKill**, was designed by [Michael Altfield (https://twitter.com/MichaelAltfield)](https://twitter.com/MichaelAltfield), a software engineer and Linux sysadmin from Orlando, Florida.

The idea is to connect the BusKill cable to your Linux laptop on one end, and to your belt, on the other end. When someone yanks your laptop from your lap or table, the USB cable disconnects from the laptop and triggers a udev script [[1](https://wiki.archlinux.org/index.php) (https://wiki.archlinux.org/index.php)

image: Michael Altfield

/Udev), 2 (https://opensource.com/article/18/11/udev), 3 (https://en.wikipedia.org/wiki/Udev)] that executes a series of preset operations.

These can be something as simple as activating your screensaver or shutting down your device (forcing the thief to bypass your laptop's authentication mechanism before accessing any data), but the script can also be configured to wipe the device or delete certain folders (to prevent thieves from retrieving any sensitive data or accessing secure business backends).

"We do what we can to increase our OpSec when using our laptop in public-such as using a good VPN provider, 2FA, and password database auto-fill to prevent network or shoulder-based eavesdropping," says Altfield. "But even then, there's always a risk that someone could just steal your laptop after you've authenticated!"

> Work in public and afraid of a "snatch-and-run"? Kill Cord for your laptop (~$20) via @MichaelAltfield (https://twitter.com/MichaelAltfield?ref_src=twsrc%5Etfw): https://t.co/2X6rrvtlji (https://t.co/2X6rrvtlji) pic.twitter.com/5lA2Qk7FdY (https://t.co /5lA2Qk7FdY)
>
> — David Bisset (@dimensionmedia) January 2, 2020 (https://twitter.com /dimensionmedia/status/1212759757100064770?ref_src=twsrc%5Etfw)

Altfield is not selling ready-made BusKill cables, at least, not for now. On his website (https://tech.michaelaltfield.net/2020/01/02/buskill-laptop-kill-cord-dead-man-switch/), the Linux IT expert published instructions on how everyone can build their own BusKill cables.

Basic components included a USB flash drive (can be empty, no need to store any data on it), a carabiner keyring to attach the BusKill cable to your belt, a USB magnetic breakaway adapter, and the actual USB cable.

The price for a cable can range from $20 to $45, depending on the BusKill configuration needed for your device and the sturdiness of its components.

Altfield also lists two sample udev scripts. One locks your device by activating the screensaver while the second shuts down your laptop.

Users will need to build their own scripts that wipe data or delete sensitive folders, as these will depend on the location and type of the data they want to delete.

Linux that fits anywhere: 15 very small footprint... (/pictures/15-very-small-footprint-linux-distros/)

SEE FULL GALLERY (/pictures/15-very-small-footprint-linux-distros/)

(/pictures/15-very-small-footprint-linux-distros/) (/pictures/15-very-small-footprint-linux-distros/2/) (/pictures/15-very-small-footprint-linux-distros/3/) (/pictures/15-very-small-footprint-linux-distros/4/)

(/pictures/15-very-small-footprint-linux-distros/5/) (/pictures/15-very-small-footprint-linux-distros/6/) (/pictures/15-very-small-footprint-linux-distros/7/) (/pictures/15-very-small-footprint-linux-distros/8/)

(/pictures/15-very-small... (/pictures/15-very-small... (/pictures/15-very-small... (/pictures/15-very-small...

1 - **5** of 16   **NEXT** > ()

SECURITY

Theoretical technique to abuse EMV cards detected used in the real world (https://www.zdnet.com/article/theoretical-technique-to-abuse-emv-cards-detected-used-in-the-real-world/)

Ransomware: How clicking on one email left a whole business in big trouble (https://www.zdnet.com/article/ransomware-how-clicking-on-one-phishing-email-left-a-whole-business-in-big-trouble/)

Best security keys in 2020: Hardware-based two-factor authentication for online protection (https://www.zdnet.com/article/best-security-keys/)

Best password managers for business in 2020: 1Password, Keeper, LastPass, and more (https://www.zdnet.com/article/best-password-managers/)

Cyber security 101: Protect your privacy from hackers, spies, and the government (https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

Phone privacy settings: Securing your iPhone and Android phone (ZDNet YouTube) (https://www.youtube.com/watch?v=92rC4x0D1B0)

Top 6 cheap home security devices in 2020 (CNET) (https://www.cnet.com/how-to/top-cheap-home-security-devices-in-2020-amazon-echo-smart-cam-wyze/?ftag=CMG-01-10aaa1b)

What are IT pros concerned about in the new normal? (TechRepublic) (https://www.techrepublic.com/article/what-are-it-pros-concerned-about-in-the-new-normal-security-and-flexibility/?ftag=CMG-01-10aaa1b)

RELATED TOPICS: HARDWARE   SECURITY TV   DATA MANAGEMENT   CXO

DATA CENTERS

By Catalin Cimpanu for Zero Day | January 2, 2020 -- 21:56 GMT (05:56 SGT) | Topic: Security

SHOW COMMENTS