

Tools for the paranoid: 5 free security tools to protect your data

Erez Zukerman | @the_ezuk
PCWorld

You just read about another online database hack, and now 4 million users' names and passwords are floating around the Internet—and you have a sinking feeling that one of them might be yours. And then there are the security breaches you don't hear about, the ones that leave nasty surprises in your inbox or on your credit card statement.

Because even a law-abiding citizen like you has a few secrets to keep, we've found five industrial-grade tools to help you hang on to what's yours. No need to enter a credit card number to get them, either—they're all free.

For hiding information in plain sight: OpenPuff

Steganography, or hiding messages in plain sight, is a storied practice dating back to ancient Greece. In modern practice, steganography means taking a media file such as an MP3 or a JPEG image and burying data in it. The file still works as usual, and if you don't specifically look for the hidden data, you'll have no idea that the encrypted information is even there. In other words, you could hide an important text message in an innocent image file, and then post that file publicly online. Another party could then download the file and—using a steganography tool and a password that you both shared in advance—process the file and extract whatever information you've buried in it. One good tool for this purpose is OpenPuff, a powerful open-source steganography application that supports a wide variety of "carrier" formats for hiding data, including MP3, JPEG, and more.

By default, OpenPuff asks you to protect your information with three different passwords, although it does let you dial that down to just a single password of your choosing. It even supports plausibly deniable encryption, and this is where things get really paranoid: Even if someone somehow realizes your seemingly innocent image or music file contains a hidden message, OpenPuff lets you hide a decoy along with the real message. Simply provide a different password, and the other person will extract the decoy out of the image, thinking they've won—but actually, your real secret will still be hidden in the file.

Steganography usually works well for hiding short text messages or other condensed information; obviously, you can't hide an entire video file within another video file using steganography—there's just no room for all those extra bytes. Still, if you need to hide a large amount of information, OpenPuff lets you chain multiple carrier files together into one extended message. To extract the information, the recipient (or yourself) needs to have all of the carrier files, and feed them into OpenPuff in exactly the right sequence, along with the correct password or passwords. Not for the faint of heart.



OpenPuff's welcome screen contains just a handful of buttons, so as to simplify what is a complex application.