CONSUMER ALERT

NATIONAL CRIME PREVENTION COUNCIL

Pirated Software May Contain Malware

You decide to order some software from an unknown online seller. The price is so low you just can't pass it up. **What could go wrong?**

Plenty. Whether you're downloading it or buying a physical disc, the odds are good that the product is pirated and laced with malicious software, or malware.

Is Your Software Pirated?

Possible signs to look for:

- ✓ No packaging, invoice, or other documentation…just a disc in an envelope
- ✓ Poor quality labeling on the disc, which looks noticeably different than the labeling on legitimate software
- ✓ Software is labeled as the full retail version but only contains a limited version
- ✓ Visible variations (like lines or differently shaded regions) on the underside of a disc
- ✓ Product is not wrapped correctly and is missing features like security tape around the edges of the plastic case
- ✓ Typos in software manuals or pages printed upside down
- ✓ User is required to go a website for a software activation key (often a ploy to disseminate additional malware)

Today, the National Intellectual Property Rights Coordination (IPR) Center (http://www.iprcenter.gov)—of which the FBI is a key partner—is warning the American people about the real possibility that illegally copied software, including counterfeit products made to look authentic, could contain malware.

Our collective experience has shown this to be true, both through the complaints we've received and through our investigations. It's also been validated by industry studies, which show that an increasing amount of software installed on computers around the world—including in the U.S.—is pirated and that this software often contains malware.

As in our above scenario, pirated software can be obtained from unknown sellers and even from peer-to-peer networks. The physical discs can be purchased from online auction sites, less-than-reputable websites, and sometimes from street vendors and kiosks. Pirated software can also be found pre-installed on computers overseas, which are ordered by consumers online and then shipped into the United States.

Who's behind this crime? Criminals, hackers and hacker groups, and even organized crime rings.

And the risks to unsuspecting consumers? For starters, the inferior and infected software may not work properly. Your operating system may slow down and fail to receive critical security updates.

But the greater danger comes from potential exposure to criminal activity—like identity theft and financial fraud—after malware takes hold of your system.

Software Buying Tips for Consumers

- ✓ When buying a computer, always ask for a genuine, pre-installed operating system, and then check out the software package to make sure it looks authentic.
- ✓ Purchase all software from an authorized retailer. If you're not sure which retailers are authorized, visit the company website of the product you're interested in.
- ✓ Check out the company's website to become familiar with the packaging of the software you want to buy.
- ✓ Be especially careful when downloading software from the Internet, an increasingly popular source of pirated software. Purchase from reputable websites.
- ✓ Before buying software off the beaten path, do your homework and research the average price of the product. If a price seems too good to be true, it's probably pirated.

Some very real dangers:

- Once installed on a computer, malware can record your keystrokes (capturing sensitive usernames and passwords) and steal your personally identifiable information (including Social Security numbers and birthdates), sending it straight back to criminals and hackers. It can also corrupt the data on your computer and even turn on your webcam and/or microphone.
- Malware can spread to other computers through removable media like thumb drives and through e-mails you send to your family, friends, and professional contacts. It can be spread through shared connections to a home, business, or even government network. Criminals can also use infected computers to launch attacks against other computers or against websites via denial of service

To guard against malware and other threats, read the tips at https://www.fbi.gov/scams-and-safety/ on how to protect your computer. If you think you may have purchased pirated software, or if you have information about sellers of pirated software, submit a tip to the IPR Center at https://www.iprcenter.gov/referral or the Internet Crime Complaint Center at https://www.ic3.gov.

And know this: Pirated software is just one of the many threats that the IPR Center and the FBI are combating every year. The theft of U.S. intellectual property—the creative genius of the American people as expressed through everything from proprietary products and trade secrets to movies and music—takes a terrible toll on the nation. It poses significant (and sometimes life-threatening) risks to ordinary consumers, robs businesses of billions of dollars, and takes away jobs and tax revenue.

Learn more by visiting the IPR Center website at https://www.iprcenter.gov and the FBI's Intellectual Property Theft webpage at https://www.fbi.gov/investigate/white-collar-crime/.

NATIONAL CRIME PREVENTION COUNCIL

Canon

National Crime Prevention Council
2614 Chapel Lake Drive • Gambrills, MD 21054
443-292-4565 • www.ncpc.org

Canon U.S.A., Inc.
One Canon Park • Melville, NY 11747
usa.canon.com/aboutcounterfeits - 1-855-46-CANON
(report potential counterfeit Canon products or sources)