Dangers of Cracked Software

You've probably heard the saying "If you're not paying for the product, you ARE the product." This couldn't be truer when it comes to cracked software. It may seem like an excellent deal – You get PAID software for ABSOLUTELY FREE and do not pay a single penny. But in fact, you are paying far more worth than money. In this module, we'll go over the dangers of cracked software and why you shouldn't install any.

1- Credential Stealing

You most likely save your accounts' credentials (e.g., emails and passwords) on your favorite browser. Well, one thing that cracked software can do is extract those credentials from your browser and all of a sudden, your account gets comprised. Often malware (i.e., bad software that steals your data) is concealed with cracked software to trick you into downloading it. While you gain the benefits of the product by using it as normal, you are getting robbed of your data and credential details.

2- Your Data Gets Breached

We assume you save important documents and files on your PC, I mean, who doesn't? That's what some cracked software wishes for – to find your important documents and steal them! The way it works is that the moment you install the software you intended to download, a malicious hidden program also gets installed on your PC. When you run the software, the malicious program runs as well and starts looking for your data and upload it to the hacker's cloud storage. The scariest part? You don't even notice it happening, and it's not easy to detect; technology is rapidly advancing and so are hackers and their tactics!

3- Ransomware Threats

Would you believe me if I told you that if you download a cracked software for the sole purpose of not paying could actually lead you to pay FAR MORE than paying for the authentic software? That's what ransomware does: It locks your files and demands a ransom to unlock them back! Nowadays, hackers come up with sneaky tactics to bundle ransomware with cracked software. When you initially run the cracked software, you instantly get hit with a ransomware attack. What a ransomware attack does is that it encrypts ALL of your files and demand you to pay them a ransom (i.e., fee) to decrypt them. Back in 2021, Colonial Pipes, the largest fuel pipeline in the US, got hit with a ransomware attack which led to widespread fuel shortages due to ceasing operations for several days. Colonial Pipeline paid a ransom of $4.4 million just to restore operations! While you could've paid $50 for the software you wanted, you now have to pay 10 times that price to get your files back. Isn't that terrifying?

4- Cryptojacking

Have you ever noticed your laptop fans getting a little too loud all of a sudden, or the laptop's performance is kind of degraded and slow? Not to scare you off, but it's probably because a hacker is using your device for mining. If you’re not familiar with cryptocurrency, it’s basically a digital currency, Bitcoin is a famous example. One of the ways to get it is to mine for them (i.e., solving very complex math problems). Mining requires capable hardware and high electricity. Hackers don’t want to waste their resources on mining, so they use yours! They bundle mining software with cracked software (specifically cracked games), so when you run the cracked software, the mining software runs as well and starts mining for Bitcoin. They often bundle them with software that require intensive processing power like video editing software and video games so that it’s hard to detect. Maybe that’s why your favorite video game is running slow on your high-end PC!

5- Keylogging and Monitoring

Imagine this: You’re now on your favorite shopping website and about to purchase something with your credit card. You insert your credit card details and hit purchase. After a few minutes, you realize someone has spent over $1000 dollars on your credit card! What happened? Safe to say that your credit card details has been compromised. While you never saved them anywhere on your device, you still typed it, and the hacker captured your keystrokes and logged the credit card details. The way it works is that cracked software can also come bundled with keylogging software that logs every single key pressed on your keyboard and send them to the hacker. In addition to that, it can also come with monitoring software that can open up your device’s camera or microphone! Are you sure you’re not being spied on right now?

Whether you’re going to pay for the actual software or download a cracked version of it, you’re still going to pay, either with money or your precious data. Our advice to avoid these types of problems is to use free alternatives for the software you want to download. That way, you don’t risk your data getting leaked or your accounts getting hacked.

-------------------------------END OF MODULE-----------------------------

-----------------------------MCQ ASSESSMENT----------------------------

1. What is the primary danger of cracked software?

a) It improves system performance.
b) It increases internet speed.
c) It often contains malware that can steal data.
d) It provides free updates.
Answer: c) It often contains malware that can steal data.

2. How can cracked software compromise your credentials?

a) By logging keystrokes and stealing passwords.
b) By deleting saved credentials.
c) By improving browser security.
d) By disabling antivirus programs.
Answer: a) By logging keystrokes and stealing passwords.

3. What hidden process often accompanies cracked software installations?

a) Malware is installed and runs silently.
b) Antivirus software gets updated.
c) Free cloud storage is provided.
d) Internet connection speed improves.
Answer: a) Malware is installed and runs silently.

4. What is ransomware designed to do?

a) Encrypt files and demand payment for access.
b) Enhance file-sharing capabilities.
c) Increase storage space on the device.
d) Improve software features.
Answer: a) Encrypt files and demand payment for access.

5. What real-world example of a ransomware attack was mentioned in the module?

a) Microsoft Hacking Incident.
b) Colonial Pipeline Attack.
c) Global Banking System Breach.
d) Cryptocurrency Exchange Fraud.
Answer: b) Colonial Pipeline Attack.

6. What is cryptojacking?

a) Logging into cryptocurrency exchanges illegally.
b) Using someone's device to mine cryptocurrency without permission.
c) Stealing cryptocurrency wallets directly.
d) Selling cracked software for cryptocurrency.
Answer: b) Using someone's device to mine cryptocurrency without permission.

7. What symptom might indicate cryptojacking on your device?

a) Reduced internet connectivity.
b) Degraded performance and noisy fans.
c) Faster processing speeds.
d) Automatic updates of cracked software.
Answer: b) Degraded performance and noisy fans.

8. How do hackers utilize keylogging software bundled with cracked software?

a) To monitor internet speed.
b) To log every key pressed and steal sensitive information.
c) To enhance software performance.
d) To improve encryption of user data.
Answer: b) To log every key pressed and steal sensitive information.

9. What additional threat can cracked software impose besides keylogging?

a) Opening up the device’s camera or microphone for spying.
b) Installing legitimate antivirus software.
c) Providing access to premium features.
d) Updating the operating system automatically.
Answer: a) Opening up the device’s camera or microphone for spying.

10. What is a safer alternative to using cracked software?

a) Using free and legitimate alternatives.
b) Downloading from unknown websites.
c) Installing multiple cracked versions.
d) Disabling the antivirus program before downloading.
Answer: a) Using free and legitimate alternatives.