THE JOURNALIST SURVIVAL GUIDE

AN ANIMATED VIDEO GUIDE

Lesson 7

How to protect your computer against hacking and malware?

Why this matters

Like building a house, it is important to make sure you have a strong foundation before building on top of it. If a computer system is riddled with malware or you have easy to guess passwords for all of your accounts, then any additional software aimed to protect data is useless.

An important first step is making sure that you have an operating system that is free of viruses and other malicious software (malware). In addition, passwords are the first step in accessing any of your content (email, social media and Skype accounts, pictures, etc.) that are stored online.

Antivirus

What is a virus?

A virus is a form of malicious software (malware) that can destroy, damage or infect the information in your computer, including data on external drives. They can also take control of your computer and use it to attack other computers. Many of these viruses spread over the Internet, using email, malicious webpages or other means to infect unprotected computers. Other viruses spread through removable media, particularly devices like USB memory sticks and external hard drives that allow users to write information as well as reading it.

Preventing virus infection

Be extremely cautious when opening email attachments. It is best to avoid opening any attachment received from an unknown source. If you need to do so, you should first save the attachment to a folder on your computer, then open the appropriate application (such as Microsoft Word or Adobe Acrobat) yourself. If you use the program›s File menu to open the attachment manually, rather than double-clicking the file or allowing your email program to open it automatically, you are less likely to contract a virus.

Consider the possible risks before inserting removable media, such as CDs, DVDs and USB memory sticks, into your computer. You should first check that your anti-virus program has the latest updates and that its scanner is running. It is also a good idea to disable your operating system›s ‹AutoPlay› feature, which can be used by viruses to infect your computer. Under Windows XP, this can be done by going inside My Computer, right-clicking on your CD or DVD drive, selecting Properties and clicking on the AutoPlay tab. For each content type, select the Take no action or Prompt me each time to choose an action options then click OK.

You can also help prevent some virus infections by switching to free and open source software, which is often more secure, and which virus writers are less likely to target.

A great anti-virus tool is Avast, which is available on both Windows and Mac devices. You can find installation instructions here: *https://securityinabox.org/en/avast_main*

Using anti-virus software effectively

Do not run two anti-virus programs at the same time, as this might cause your computer to run extremely slowly or crash. Uninstall one before installing another.

Make sure that your anti-virus program allows you to receive updates. Many commercial tools that come pre-installed on new computers must be registered (and paid for) at some point or they will stop receiving updates. All of the software recommended here supports free updating.

Ensure that your anti-virus software updates itself regularly. New viruses are written and distributed every day, and your computer will quickly become vulnerable if you do not keep up with new virus definitions. Avast will automatically look for updates when you are connected to the Internet.

Enable your anti-virus software›s ‹always on› virus-detection feature if it has one. Different tools have different names for it, but most of them offer a feature like this. It may be called ‹Realtime Protection,› ‹Resident Protection,› or something similar.

Scan all of the files on your computer regularly. You don›t have to do this every day (especially if your anti-virus software has an ‹always on› feature, as described above) but you should do it from time to time. How often may depend on the circumstances. Have you connected your computer to unknown networks recently? With whom have you been sharing USB memory sticks? Do you frequently receive strange attachments by email? Has someone else in your home or office recently had virus problems? If any of the answers to these questions is “Yes”, you should scan your system as soon as possible.

Antispyware

What is Spyware?

Spyware is a class of malicious software that can track the work you do, both on your computer and on the Internet, and send information about it to someone who shouldn›t have access to it. These programs can record the words you type on your keyboard, the movements of your mouse, the pages you visit and the programs you run, among other things. As a result, they can undermine your computer›s security and reveal confidential information about you, your activities and your contacts. Computers become infected with spyware in much the same way that they contract viruses, so many of the suggestions above are also helpful when defending against this second class of malware.

Preventing spyware infection

Stay alert when browsing websites. Watch for browser windows that appear automatically, and read them carefully instead of just clicking Yes or OK. When in doubt, you should close ‹pop up windows› by clicking the X in the upper right-hand corner, rather than by clicking Cancel. This can help prevent webpages from tricking you into installing malware on your computer.

Never accept and run this sort of content if it comes from websites that you don›t know or trust.

To routinely counteract spyware infection, we recommend using the anti-spyware tool Spybot, which scans your computer (much like an anti-virus program) and safely removes spyware that can track your activities conducted on your computer.

Passwords

How to create a stronger password

A good password should have the following characteristics:

Length: at least 8 characters

Strength: diversity of characters (use different letters, incorporate symbols, and change case)

Rotation: changed on a semi-regular basis

You should more frequently rotate passwords on more important accounts (Facebook, email, etc).

Uniqueness: do not repeat the use of passwords

One way to help remember this is by using a multi-word “passphrase”-consisting of 4 or more random words.

Even with a slightly easier-to-remember passwords, it's nearly impossible to remember a unique password for all of the websites you have accounts for. Thus, using a free and open source password manager like Keepass can make this job easier for you.

Keepass can store all your passwords including your computer's admin password, so that you can make any necessary updates if prompted by the system for an update. In addition, the "copy and paste" from Keepass protects your passwords should your machine be compromised by key loggers or other types of malware.

Produced by:
The SKeyes Center for Media and Cultural Freedom at the Samir Kassir Foundation

The content of the video was prepared with the pro bono assistance of:
The ICT team at the National Democratic Institute

Executive producer: **Maroun Sfeir**
Storyboard creation and animation: **kook creative studio**

Video Consultant: **Andrew Codd**
Translation: **Nour El-Assaad**
Voice over - Arabic: **Rima Khaddaj**
Voice over - English: **Andrew Codd**
Sound recording: **Creative Impact**
Music: **"Mining by Moonlight" by Kevin MacLeod**

This project has been made possible thanks to the support of the **National Endowment for Democracy**.