

# How To Protect Yourself Online from Malware & Phishing Attacks

## Who Are We:

The National Telecom Regulatory Authority (NTRA) was established in 1998. The NTRA's legislative and regulatory framework has been defined pursuant to the Telecom Regulation Law No. 10 of 2003, that stipulated that the NTRA is a national authority competent to regulate and manage the ICT sector on the basis of fundamental principles, including, transparency, free competition, universal service, consumers' rights protection and non-monopolistic practices.

Chief among NTRA's goals are the provision of high-quality telecom services at the most affordable prices, in addition to the exertion of all efforts to enhance the services, keeping abreast of the state-of-the-art technologies and huge advancements in ICT field. Thereupon, and in implementation of NTRA's main goals, the Consumers Rights Protection Committee (CRPC) was formed in August 2004. It allows all telecom service users to communicate and interact directly with all telecom users by launching awareness campaigns and taking various measures. The CRPC, chaired by NTRA's Executive President, comprises notable public figures and convenes regularly.

In order to activate and fulfill the rights of every user to be provided with high-quality services, get clear and all-inclusive information about them and obtain health and environmental parameters, the NTRA established the Call Center. NTRA's Call Center receives complaints, inquiries and technical complaints of service failure from all users in the A.R.E., through the hotline (#155) and the free number (08003330333). It acts as a second-tier or second level for examining and solving such complaints, around the clock, in case the subscriber does not have his problem solved by the service provider.

To know the latest and most important ICT news on the local and international levels in addition to all issues related to the telecom market in Egypt, you can visit NTRA's website: [www.tra.gov.eg](http://www.tra.gov.eg). You can also address the NTRA through the following address: Smart Village, B4, K 28 Cairo-Alexandria Desert Road, Giza, A.R.E.,

Tel; (+202) 35344000;

Fax: (+202) 35344155;

Email: [info@ntra.gov.eg](mailto:info@ntra.gov.eg)

Youtube: <http://www.youtube.com/user/CRPCNTRA>

Facebook: <https://www.facebook.com/CRPC.NTRA>

Twitter: <https://twitter.com/crpcntra>

## Protect Yourself Against Malware:

When you use a certain computer, you have to protect yourself from malware, or “malicious software”, that is a software specifically designed to access or damage a computer while the user is unaware of it. There are various types of malware, including spyware, key loggers, viruses, worms, or any type of malicious codes that hack and infiltrate a computer.

Generally, it often happens that the device becomes hacked with malware as the user, unknowingly, installs it on his device. The malware only works if the computer runs continuously without being shut down. Malware works, like most spams that require some conscious or unconscious help from its victims. The question is: how do you end up downloading and installing a malware?

Sometimes a malware is bundled with a licensed software package, at other times, the user simply clicks on a fake message that can trigger a malware download. Hence, the most common way for a malware or virus to enter a computer is via an email attachment. We recommend you to strictly adhere to the following tips and learn how you can protect yourself from malware:

- **Be mindful of the websites you are visiting:** many websites that host harmful content will use pop-up ads that apparently seem to be error messages or offering prizes to the user. When you visit these websites, the harmful content is downloaded into your computer. That is why you have to avoid being tempted by this in the first place.
- **Be cautious of what you are downloading:** do not download software from a website that is replete with advertisements, or lists of 'free' programs, these are often fake files. Be cautious, question it, and check it with a security software before opening or downloading programs. You should always download programs from reputable websites or corporates.
- **The Purchase of security software:** many users are not aware that using pirated software cannot protect their computers against threats and the third party's pirated software that may contain viruses.
- **Take extra care when using Peer-To-Peer programs:** since the files shared on P2P networks are not policed, anyone can release anything they want through them. Hence, you have to scan the files you have downloaded before executing them.
- **Accepting the attachments incoming to your email as expected:** some threats can damage machines and automatically send copies of themselves to the user's contact list. It might appear to you that your friend is sending you an attachment but you realize later on that it is nothing but a malicious program propagating itself.

- **Know the File Formats:** images usually come in (.jpg, .jpeg, .png, .bmp, .gif, and .tif) formats. Executable files come in (.exe, .bat, .com, .dll) extension. If someone tells you that he will send you a photo but the file ends with (.exe) or (.com) extension, then do not open it because they will potentially endanger your machine.

## Cybercrimes and preventive measures that must be Taken Spam emails (information you need to know):


- ✚ **What is a “spam”?** A “spam” is a common term for junk emails (unwanted and unsolicited messages) sent to your email account or mobile phone. Some spams promote a product or invite you to visit a website; other spam emails try to deceive and convince you to invest in some fraudulent plans or reveal your bank account or credit card information. These emails usually carry viruses and malware.
- ✚ **How can I tell if a message is a spam?** In case you receive any commercial message sent to your email or mobile phone that does not meet the following conditions:
  - **The receiver’s consent:** it must be sent after obtaining your consent, either expressly or implicitly by inferring it from any business activity or other relation between you and a certain company.
  - **Accurate data:** it must contain accurate information about the person or company that sent it.
  - **Unsubscribe:** it must contain the ‘unsubscribe’ function that enables you to choose not to receive such messages from that source.
- ✚ **What can I do if I receive a “spam” message?** Some spam messages are sent by professional spammers locally and globally, whereas other spams are sent by legitimate companies. If you receive commercial messages via email or mobile phone, you have many options to respond to it.
- ✚ **Do not ever respond to an email that seems deceptive or dubious:** If you receive an email that seems to you deceptive or dubious, or its topic or sender looks suspicious, it will be safer to delete it immediately without opening it. Do not reply to it, or click on any links, including the ‘unsubscribe’ links, as this might result in receiving more spams.
- ✚ **Do not buy spam-advertised products or services as many of them are fraudulent.** If the source of these emails or messages seems genuine, contact the company to make a complaint. You may contact it by phone or in writing, to make a complaint and ask it to delete your email from its mailing lists.


## Online Social Networking- How to be Safe Online:


Online social networking or using web-based services to interact with people about shared activities or interests can be a great way to pursue interests, establish and enhance existing friendships, play games, and share ideas. While interacting online has many benefits, posting too much personal information in an online personal profile, blog or chat can be risky. The careless behavior of the user can lead to the damage of his reputation from the unintended use of his personal information or becoming a victim of fraud, identity theft, scams and harassment.


### **To Reduce Online Risk:**


- You have to control who has access to your information.
- Think carefully before you give personal information (such as your name, age or postal address) or your financial details (especially the credit card or bank account details).
- Set up and check online privacy and security settings when you create a personal profile to make sure you know who can access your information.

 **Damage to Reputation:** information or images posted in the user's online profile, blog or website can be used, or taken out of context in order to embarrass you and damage your reputation. Remember that any information available about you online might remain published and available forever. You can verify the information about you that is publicly available online by typing your own name into a search engine.

 **Online Fraud and Identity Theft:** the more information you provide online, including the social networking profiles, photos, posts and live chats, the easier it is for criminals to use your details to steal your money or identity. That is why you should limit the personal information you share online and before publishing any of your personal information.

 **Cybercrimes:** impostors and fraudsters succeed with their online fraudulent methods because they offer things and products that individuals and users want, such as gaining a huge amount of money without exerting any effort, then you should not respond to any unexpected offers or requests in exchange you're your personal or financial information when using social networking sites.

 **Electronic Harassment:** when your personal information is posted publicly, it can be used by others to harass or threaten you. You must always keep your physical address and location private and confidential. You must think carefully about publishing names, photos showing car licence plates, street names and venues that you frequent in a way that can be easily linked to you.

 **Keeping Children Safe Online:** internet users are responsible for the amount of information they reveal online. It can be used for other purposes that they have not expected. You can help your children stay safe online by reminding them of the following:

- Do not ever share passwords, no matter how much they trust their friends.
- Use strong passwords consisting of a combination of letters and numbers
- Do not publish your children's personal details, especially photos.
- Block senders of inappropriate or annoying messages or delete them from their contact list.
- Do not give their mobile numbers to people they do not know well.

**For Mobile, Internet and Fixed Service Users:**

If you have encountered a problem with the service provider and could not solve it, call the Call Center hotline (155) and we will exert all efforts to solve your problem. The Call Center receives complaints and inquiries on a daily basis throughout the week.