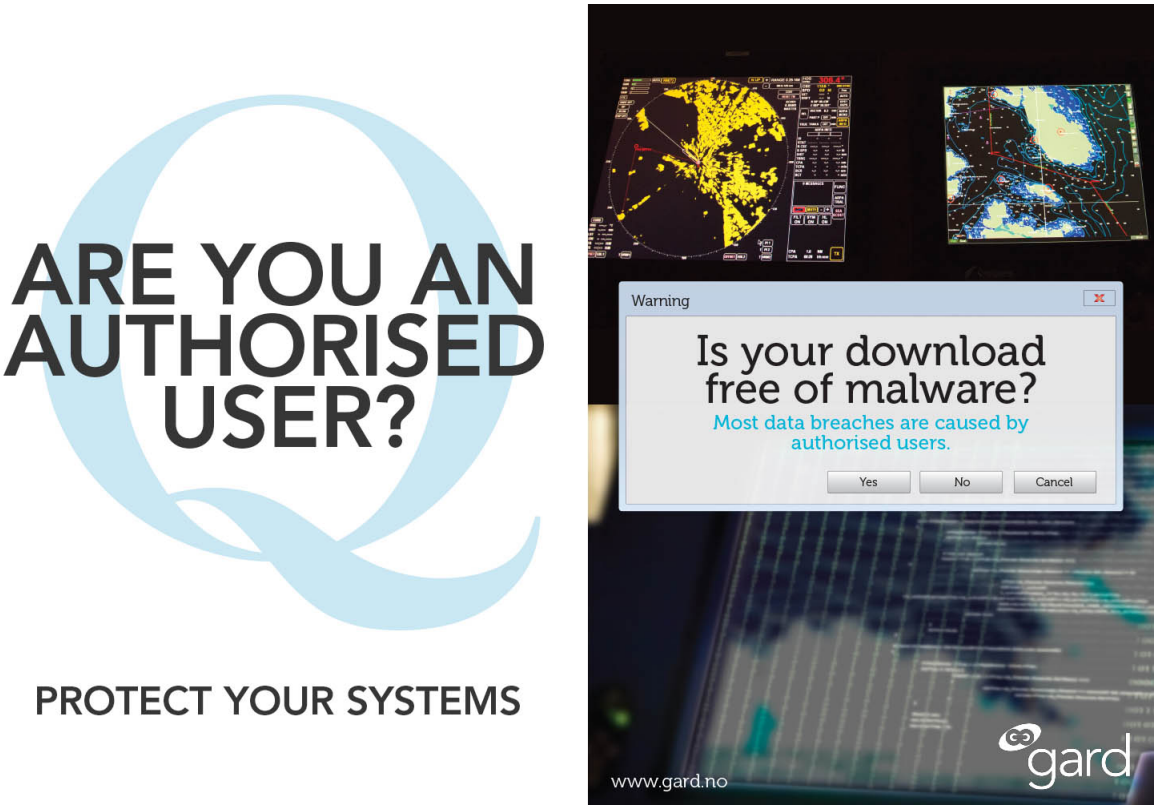

Stop malware finding its way onto your computer systems

Malware, short for malicious software, is designed to damage files or entire computer systems, steal data, or disrupt networks. Malware can be viruses, worms, Trojans, spyware, adware, backdoors, rootkits, and bots. There are numerous inexpensive Antivirus software programs available to protect your IT and OT systems from malware, but first line of protection is knowing how malware spreads so you can avoid it in the first place.

Published 29 October 2019

Malware will enter your computer in one of three ways:

• As a download from a web page:
If you use the latest version of your web browser, you will be alerted to any download from a web page onto your computer. In other words, you must invite the program into your realm and if that program is malware, in it comes.

• As an email attachment:
Malware arriving in the form of an email attachment is the same bad stuff that comes from a web page. The difference is primarily in the way an attachment uses social engineering: The malware is often disguised as a message from a friend, your employer, your bank or your business contact or has another tempting aspect that entices you to open it.

• As a file on infected removable media:
Originally the most popular method of malware distribution, inserting a USB-stick or another type of media into your IT or OT storage system is still a way to infect your computer with a virus. Never ever start a PC or computer system with a USB-stick inserted.

The key to getting malware to work is social engineering. In the case of a web page link, the web page may direct you to ignore warnings from Windows or to disable your antivirus software to continue.

Recommendations

• If the website does not look quite right, or if is offering something that cannot possibly be true, it may be best to avoid downloading any of its files or even click a link.

• If a file downloads automatically and you did not request it, do not open the file and delete it at once.

• If a pornographic website downloads a “video viewer,” it is a virus.

• If the email says to disable your antivirus program before opening the attachment, don’t.

• It has recently become more common to be infected with malware through messaging services and chat rooms, like WhatsApp, Messenger, LinkedIn, Facebook and Twitter. Fake user account tries to become friend with you and sends you a web page link to malware, often with an enticing but wrong description of what you find when you click the link. Do not click the link!

Whatever you do, however you’re tempted, do not click a suspicious link or open an untrusted file!

Additional material

Cyber security awareness package (provides links for posters, presentations, case

correspondents, or other contributors.

studies and videos)

Alert Maritime industry targeted by cyber criminals

Alert Ship operators cannot afford to turn a blind eye to cyber security

Insight Cyber security awareness in the maritime industry

Insight It is time to strengthen your onboard cyber security procedures

Videos

Gard%20Case%20study%20Cyber%20security.pdf

Loss Prevention Poster Cyber security

Loss Prevention Poster Think before you click

Loss Prevention Poster gard_poster16_++malwarefree_lores+%28ID+367618%29.pdf