

INTERNET WORM



Worms are a form of malware that replicates across the Internet or local networks.



Worms differ from computer viruses because they can propagate themselves, rather than using a carrier program or file. They simply create copies of themselves and use communication between computers to spread.

The Conficker worm is an example of an Internet worm that exploits a system vulnerability to infect machines over the network. Such worms are capable of spreading very rapidly, infecting large numbers of machines.



Some worms open a “back door” on the computer, allowing hackers to take control of it. Such computers can then be used to send spam mail.

Best Practices

1. Be sure to install antivirus software.
2. Always keep antivirus updated.
3. Remember to patch your computer regularly.
4. Always scan external storage devices for malicious software
5. Do not open unwanted emails and attachments.
6. If files and folders will be shared, remember to password protect them and use password complexity.



For comments or inquiries email infosec@pjlhuillier.com

-- End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCES:

- Sophos Ltd. (2012). Threatsaurus: The A-Z of computer and data security threats.
- [Apr032009 Release13 InfoSec101 Stay Immune.pdf](#)