Nov 28 2014 Release # 294

-- Begin Transmission --

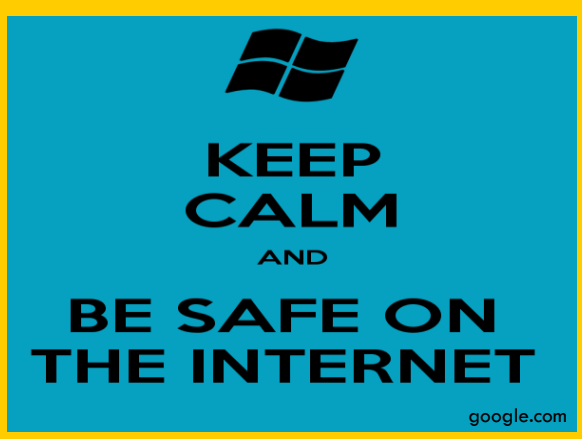
Keep up-to-date with security patches

Hackers frequently exploit vulnerabilities in operating systems and programs in an attempt to infect computers. Be aware of security updates for your computer's operating system, browser, plugins and other code that could be the target of hackers. If you can, set up your computer to automatically download security patches.

google.com

google.com

google.com

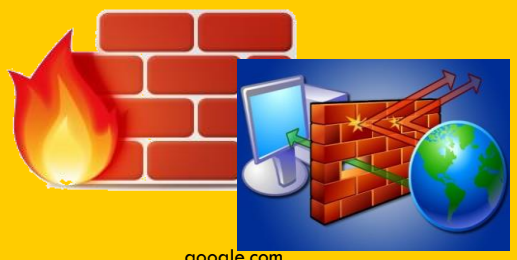


google.com

How to be safe on the internet

Use firewalls

A network firewall is installed at your organization's boundary and admits only authorized types of traffic. A client firewall is installed on each computer on your network, and also allows only authorized traffic, blocking hackers and Internet worms. In addition, it prevents the computer from communicating with the Internet via unauthorized programs.



google.com

google.com

Don't follow links in unexpected emails

Links in unexpected emails can take you to bogus websites, where any confidential information you enter, such as account numbers and passwords, can be stolen and misused. In addition, hackers often try to direct you to malicious webpages by spamming out links via email.

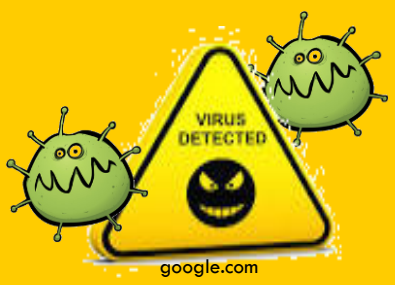
Use different passwords for every site

You should use a different password for each site where you have a user account. That way, if a password is compromised, only one account will be affected. In addition, make sure that your passwords are hard to guess and never use a dictionary word as your password.

google.com

Scan email for malware and spam

Anti-spam programs can detect unwanted email and prevent it from reaching users' inboxes, as well as scan for malware contained within the email.



google.com

google.com

Use routers

You can use a router to limit connections between the Internet and specific computers. Many routers also incorporate a network firewall.

Information Security. It's a Shared Responsibility

REFERENCE(S): https://www.us-cert.gov