# Proper Email and Internet Procedures

In response to recent events concerning the virus on the clinic's computer system, we want to educate all staff members on proper email and internet procedures to increase computer security. These measures are beneficial for both work and home!

## Email

Today we typically access email directly through a computer email program or online. Both have the potential to expose a computer to malware and/or virus.

- Email hackers/spammers are incredibly creative in making spam email appear legitimate. Common scams include: IRS trying to issue you uncollected tax refunds, FBI trying to track you down, FedEx/UPS unable to deliver a package, company needing you to verify information, relative trying to send you money, a company contacting you about an order (that you did not place).
- ***Extreme discretion should be used when checking emails.***
- NEVER open an email, attachment or click on a web link in an email unless you know 100% who the email is coming from <u>and</u> you are expecting the email and its contents and have reasonable confidence the information is safe. Simply because you recognize the name in the email does not make it safe. Email accounts are often hacked and used to distribute spam email to people in a person's contact list.

## Internet

The clinic computers are solely for the purpose of conducting clinic business. At times, staff may need to use the internet to verify a check payment, process a Care Credit application, and similar business-related reasons.

- ***Extreme discretion should be used when accessing websites.*** We access so much information from the internet that we can mistakenly develop a false sense of security about the internet.
- NEVER go to a website that you are not familiar with its safety. NEVER download a file from the internet without permission from management. (Clinic documents on the clinic's website Resources page have permission unless appears abnormal.)
- The clinic uses a virus protection program and site advisor. However, these safety measures only work if the user heeds the warning(s). If you receive a warning message, do NOT proceed to the website! Also, should you need to do an online search for clinic-related purposes, be sure you are only accessing websites that have a site advisor green check mark next to them. While this doesn't guarantee the site is completely safe, it does minimize the risk.
- Be wary of pop-ups that indicate a computer problem and want you to click on the screen to run a scan (or any other pop-up that requests an action). This is usually a form of phishing (attempt to defraud someone by appearing as a legitimate company) and could infect the computer with malware or a virus.
- Free Wi-Fi is not safe Wi-Fi. Never access or input personal information on an unsecured Wi-Fi connection. Treat such Wi-Fi as posting a memo for anyone to see. You also risk someone accessing/affecting your computer or personal electronic device.

***If ever in doubt about an email or internet site, do NOT access--ASK management first!***