CRITICALLY IMPORTANT INFORMATION FROM I.T.!

Top Ten Things You Need to Know About Phishing and Malware

➤ Only open email attachments if you’re expecting them and you know what they contain.

➤ Never click a link to increase your email quota. That is always a scam.

➤ Never open emails or click on links that ask for your personal information.

➤ Never enter your personal information in a pop-up screen.

➤ Be suspicious of emails with urgent requests for personal financial information. These are always scams.

➤ Know that phishing can also happen by phone. You may get a call from someone pretending to be from a company, I.T. or government agency, making false claims and asking for your personal information.

➤ Beware of browser malware. If you start to see lots of pop-ups in your web browser, your machine is likely infected.

➤ Only communicate information, such as credit card numbers or account information, via a secure website or the telephone (HTTPS for the web).

➤ Use a different and strong password for your work and personal accounts.

➤ If you see unusual behavior, call I.T.!

508.373.1999