PROTECT YOUR SYSTEMS FROM CYBER THREATS!

**July 20, 2017**

**TIMED OUTLINE**

This course was developed to meet the education training requirements and provide students with 1 hour of continuing education.

**Course Overview:** You’ve read the headlines lately about cyber-attacks and that they are at an all-time high. Every day there is another story of a hack against an un-ending list of companies like Target, Home Depot, Sony, Anthem, etc.  While those make the headlines, did you know that 62% of all cyber-attacks are against small to medium sized organizations that you don’t hear about in the news?  Have you seen the growing trend of cyber-attacks targeting human resources personnel and other key employees at companies?

One-third of organizations that are the victims of a cyber-attack go out of business within six months. Are you prepared to protect your data—client information, financial data, contacts, other items and files stored on your computers and servers?  Learn how to be proactive to protect yourself and your company from ransomware, phishing, spear-phishing, spamming and other types of cyber-attacks in this can’t miss webinar

**Learning Objectives:** Upon completion of the course, the participant will know:

* The five steps to protecting your organization from Cyber attacks.

**PRESENTER:**

**Jack McGrath**

Jack McGrath is president of Digitec Interactive – a training provider who has been designing and developing interactive learning since the 1990s and is nationally recognized for eLearning course design, including security courses for ISACA, Cisco Systems, Go Pro and others. Jack is the inventor of NetDefense Pro – an online cybersecurity education platform, designed to keep the bad guys out of your systems.

**TIMED OUTLINE**

1. **Intro (5 Minutes)**
   1. Today’s presenter
   2. Statistics
2. **What is phishing? (10 Minutes)**
3. **What is ransomware? (10 Minutes)**
   1. Be skeptical. Is this a phishing scam?
   2. Are there any red flags in this email?
   3. Does it look legitimate?
   4. How can you tell?
   5. What do you look for?
4. **Be a Human Firewall (10 Minutes)**
   1. What is a social engineering scam?
   2. Social media mining
   3. Think like a “firewall”
   4. Reinforce password security
   5. Consider a password manager
   6. USB drives/sources of malware
   7. Public connections
5. **Cybersecurity training (10 Minutes)**
6. **Recap/Q & A (15 minutes)**