**Cyber Security**

The threat of cyber-robberies targeting small companies, local governments, school districts, churches and non-profits continues and is increasing. That threat is very real and has victimized numerous Maine companies.

A typical threat begins with an innocent looking e-mail received by an employee. When the employee clicks on the e-mail malicious malware is launched whose purpose is to steal access to their on line banking.

Several instances of this type of theft have occurred in Maine, often with disastrous results for the company.

We are advising our clients to follow strict practices to combat fraud and we refer them to United States Computer Emergency Readiness Team for guidance on how to protect themselves from this type of theft.

The following practices and Cyber Security Guidance is provided by the United States Computer Emergency Readiness Team [www.us-cert.gov](http://www.us-cert.gov/).

**Management & IT Department**

* Implement Defense-in-Depth: a layered defense strategy that includes technical, organizational, and operational controls. Use a secure dedicated computer for all banking transactions.
* Establish clear policies and procedures for employee use of your organization's information technologies.
* Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
* Update your anti-virus software daily.
* Regularly download vendor security "patches" for all of your software.
* Change the manufacturer's default passwords on all of your software.
* Monitor, log, and analyze attempted intrusions to your systems and networks.

**Employees**

* Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
* Change your passwords regularly (every 45 to 90 days).
* Do NOT give any of your user names, passwords, or other computer/website access codes to anyone.
* Do NOT open e-mails or attachments from strangers.
* Do NOT install or connect any personal software or hardware to your organization's network hardware without permission from your IT department.
* Make electronic and physical back-ups or copies of all your most important work.
* Report all suspicious or unusual problems with your computer to your IT department.
* Create a mobile device action plan if their devices have access to your network.
* Maintain back-up copies of your business network data.
* Secure your Wi-Fi networks.
* Limit employee access to data and information and limit authority to install or modify software.
* Control physical access to your network and business computers.
* Limit information stored on laptop computers and mobile devices.

To read more about the ways to protect yourself against cyber security go to[www.US-CERT.gov](http://www.us-cert.gov/).  You can sign up to receive technical and non-technical cyber alerts.

The University of Southern Maine has developed a Small Business Cyber Security Guide to give business owners a reference on protecting their assets. The guide can be found at [www.maine.gov](http://www.maine.gov) and searching Small Business Cyber Security Guide.

This list of suggestions is not intended to be a comprehensive defense against the threat of cyber-crime. Please consult your cyber security expert or contact us for a referral to a qualified expert.

 

***Katie Zenko, CPA***

207.956.6708

[kzenko@btr-cpa.com](mailto:kzenko@btr-cpa.com)

***Michael C. Royer, MST, CPA***

***President***

207.956.6704

[mroyer@btr-cpa.com](mailto:mroyer@btr-cpa.com)

 

“***Big enough to serve, small enough to care"***