Get our Network Security Report here

IT Security Tip #24: How to keep staff from unintentionally causing a security breach

With so many access points, from cell phones to laptop and home computers, how can anyone hope to keep their network safe from hackers, viruses and other unintentional security breaches? The answer is not “one thing” but a series of things you have to implement and constantly be vigilant about, such as installing and constantly updating your firewall, antivirus, spam-filtering software and backups. This is why clients hire us – it’s a full-time job for someone with specific expertise (which we have!).

Once that basic foundation is in place, the next most important thing you can do is create an Acceptable Use Policy (AUP) and TRAIN your employees on how to use company devices and other security protocols, such as never accessing company e-mail, data or applications with unprotected home PCs and devices (for example). Also, how to create good passwords, how to recognize a phishing e-mail, what web sites to never access, etc. NEVER assume your employees know everything they need to know about IT security. Threats are ever-evolving and attacks are getting more sophisticated and clever by the minute.

This e-mail series is one great way to keep your employees informed, but you STILL need a good AUP in place and training. If you’d like our help in creating one for your company, based on best practices, call us at 907-885-0500 or reply to this e-mail. You’ll be glad you did.

If you would like your employees to opt in for these security tips and download a free report we’ve recently published on protecting yourself from cybercrime, forward this link to them:

http://www.dantechservices.com/cybersecuritytips/

If you have any questions, just click here to reply to this e-mail or call me at **907-885-6518.**

Sincerely,
Dan Foote, President
DanTech Services, Inc.