October is National Cyber Security Awareness Month!

The Department of Homeland Security has designated October of each year as National Cyber Security Awareness Month. This is an annual campaign to raise awareness about cybersecurity. We live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not. National Cyber Security Awareness Month (NCSAM) is designed to engage and educate public and private sector partners through events and initiatives to raise awareness about cybersecurity. It will also provide tools and resources needed to stay safe online, and increase the resiliency of the Nation in the event of a cyber incident. (source: DHS website)

NCSAM 2016 Weekly Themes

Week 1: October 3-7, 2016 – Every Day Steps Towards Online Safety with Stop.Think.Connect.™

Week 2: October 10-14, 2016 – Cyber from the Break Room to the Board Room

Week 3: October 17-21, 2016 – Recognizing and Combating Cybercrime

Week 4: October 24-28, 2016 – Our Continuously Connected Lives: What's Your 'App'-titude?

Week 5: October 31, 2016 –Building Resilience in Critical Infrastructure

Please visit the NCSAM Resources page to find the 2016 NCSAM One Pager with information about the weekly themes. (source: DHS website)

Why would anyone want to hack a local utility company?

Hackers often target small to medium size companies of all kinds. This is because many are not as sophisticated in their approach to cyber security as a larger company might be.

We all know of the increasing risks of cyber security breaches to the national power grid. The Ukraine power grid breach and many other events have heightened our awareness of what the "bad guys" are capable of doing to our critical infrastructure.

But the potential for damage extends far beyond that. All of our businesses have sensitive data that is valuable on the "dark web." Hackers can profit by stealing and selling much of the information tied to our financial systems. Credit card account information, bank draft information, employee social security numbers, all have value to be sold for identity theft. Undetected access to our systems and networks can also give thieves a place to hide and conduct their business. A hacker might not want to steal your data. They might just shut your systems down until you pay a "ransom" to restore them.

We tend to think that most of the hackers operate outside of our country, but there is an increasing amount of activity coming from inside of the U.S. border. These domestic hackers may even be locals who have some knowledge of our personnel and how we operate. They can even be former or current employees.

Start with the basics -

National Cyber Security Awareness Month is the perfect time to evaluate your policies, processes and employee education on cyber security.

We can never assume that we are finished with securing our data and systems. It is an ongoing process to be practiced, re-evaluated and reinforced. Cyber security policy and processes must be measured, assessed and communicated to our employees on a regular basis.

Do you have good policies in place?

Have your systems been tested or audited recently?

Do you know what to do when a breach happens?

Are employees trained regularly?

These are critical questions that you should have answered.

The Weakest Link…

No one wants to be the cause of a data breach for themselves or their company. But the truth is, even if we have good policies, processes, and tools for cyber security, the greatest risk is in human error. It is critical to educate and reinforce the knowledge of employees with security awareness training.

Employees must be trained on good daily habits, like using more secure passwords and protecting them. We must also alert them to the social engineering approaches that bad guys use to get information over the phone, and how the wrong mouse click on an e-mail can give someone access to your systems, or introduce a virus or ransom-ware.

Training Resources for TMEPA members

In support of National Cyber Security Awareness Month, SecurIT360 is providing complimentary access to online Security Awareness Training content for TMEPA members in October.

If you would like to take advantage of this, contact –

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250