You Have Been Hacked!

Chances are high that you or your housing authority have been hacked. You probably don't realize it and you are potentially continuing to leak private information about you, your tenants, and your employees.

- **According to US government statistics, in 2016, the number of ransomware attacks increased 300 percent from 2015, with over 4,000 attacks detected per day.**
- **Most internet users can answer fewer than half the questions correctly on a knowledge quiz about cybersecurity issues and concepts. –** Pew Research Center
- **86 Percent Increase in Data Breaches in 2016 Led to 1.4 Billion Data Record Compromised…The leading type of breach is related to identity theft.**

Massive data breaches at companies like Yahoo and Target make headlines around the world. Yet, the security threat does not just come from malicious outsiders. It very frequently, comes from people within an organization who by accident or on purpose release sensitive information to unauthorized parties.

According to a recent study by BPI and FoxIT Software, there is "a glaring lack of effective security practices surrounding the way companies create and share confidential and sensitive documents. The result is that a wide range of high-value, confidential information is routinely at risk in businesses and government agencies today."

Study Highlights:

- Almost three-quarters of respondents say their organizations produce sensitive or confidential documents on a weekly or more frequent basis.
- Over 61 percent say their organizations lack effective document security.
- The number one document security challenge, by far, is accidently sending a confidential document to the wrong party.
- Close to six in 10 people say they or someone they work with have mistakenly sent out documents they shouldn't have.
- The vast majority of respondents believe increased connectivity and proliferation of devices have increased document security challenges in their organization.
- Respondents point to a wide range of repercussions for document leaks— from reputational damage and competitive risks, to lawsuits, lost revenue, lost time and job loss.
- 87% of senior managers admit to regularly uploading work files to a personal email or cloud account

Employees are often the weakest link in an organization. Hackers use social engineering to trick users into clicking on infected advertisements or URLs in emails or into downloading attachments that will infect the corporate network with ransomware.

Employees are the most common entry point for hackers seeking a way into your organization, so **regular security training** to educate them about network security and risk detection may reduce malware infections. Quite often the malicious code is implemented on legitimate websites to trick the untrained. The workers must learn to distinguish between authentic links, emails, and phishing scams which could lead to viruses, ransomware infections or trick them into giving away passwords and sensitive information.

Multi-purpose devices used for both home and work tasks are a top risk. It only takes one random click to get infected. Once the device is connected to the company network, the infection can spread to the entire company network.

Hackers don't always need to expend much effort in breaching your network because you make it easy for them from the start. Many users do not have good passwords and often reuse their passwords. Using "free" email accounts puts your information at higher risk. Most small offices do not have proper business quality network equipment, security software and properly maintained computers. You should perform regular updates of all software, and check them for vulnerabilities. Most offices are not prepared and usually lack the skills to perform the routine maintenance, much less research and stay on top of these new threats.

Implement multiple prevention methods to lower the risks at your housing authority -- it's always cheaper to prevent ransomware attacks, data losses and viruses than to spend money on recovering data and fixing problems afterward.

You need Business class tools; such as business email with spam protection and real-time scanning of content, network equipment that protects everything on your network and monitors for unusual activity, security software that stops multiple types of threats and alerts when there is a problem, monitoring and management software that scans, updates and monitors for vulnerabilities on your computers and finally a good solid backup plan.

Remember, your computers are tools, not toys. Housing Authorities are a business, treat your technology like business tools and take proper care of them. This will make your work safer and more productive.

Measure Your Security Risk

Answer Yes or No to the following questions. Yes=1 point, No=0 points

1. Do you use Yahoo or other "free"email
2. Do you use USB sticks or flash drives
3. Do you use hotel, coffee shop or other public wifi when travelling?
4. Do you let people connect to the wifi at your office?
5. Do you ever use your personal email for work?
6. You do not have a security training process?
7. Do you have a shared documents folder on one of your office computers?
8. Is your networking equipment limited to what your internet provider gave you?
9. Do you reuse the same password(s) on any of your online accounts?
10. Is your home page set to MSN, Yahoo or other "news" site?

If you answered Yes to more than 3 of these questions you are at an increased risk of losing personal information related to your housing authority.

Ask about our Security Assessment Process. We remotely perform an assessment of your current computers and network then produce an action plan of what needs to be addressed.

Call or email to find out how we can help you with the issues mentioned in this document.