



# HACKTIVISM, AND THE REAL RISK FOR MUNICIPALITIES AND WATER DISTRICTS

**H**acking! No, we're not talking about the kind of cough that seems to start going around this time of year. We're talking about a cybercrime – breaking through security in a computer system. While many “black hat” hackers force their way into large information networks for the purpose of stealing sensitive information or sabotaging a company, a relatively dormant subgroup of hackers is now growing, breaking into computers with the intent to raise awareness for their particular cause. A portmanteau of the words “hack” and “activism”, the term “hactivism” refers specifically to hacking for a politically or socially motivated purpose. In her 2004 dissertation “Hactivism and the Future of Political Participation,” Alexandra Samuel defines it as: “...The nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development.” In 1996, the term was first coined by a member of Omega, a Cult of the Dead Cow hacker collective.

While the activity is the same as regular hacking, the intent is different. Hactivists use the same tricks, such as disrupting services, launching denial-of-service attacks, or posting an overt alternate file or

redirect. For example, a hactivist might be disgruntled over a city regulation and create a message on a webpage touting their dissatisfaction that displays instead of the city's homepage on their Web site.

Victims of hactivism are not limited to larger targets, however. A group of hactivists calling themselves “Anonymous” broke into 70 individual, small, rural law enforcement systems in August 2011, compromising sensitive data and crime tips, according to the Associated Press. This cyberprotest defaced

Web sites in an attack against police who had been pursuing and arresting members of the Anonymous hactivist group. Smaller municipalities, counties, or rural water districts who cannot afford IT departments are easier targets because their systems generally less secure,

and data is housed in a single location, making a system-wide catastrophe possible in one hit.

Hactivism is not a recent phenomenon. In 1989, the first recorded act of political hacking occurred when the anti-nuclear WANK worm invaded NASA computers. The welcome screen displayed the message: “Your computer has been officially WANKed. You talk of times of peace for all, and then prepare for war.” But until recently most hactivism attacks were aimed at large, federal or state organizations. Local and rural entities are now being seen as easy prey.

**Local and rural entities are now being seen as easy prey.**

## Ugh? Hack us? No way!

The highest obstacles in the emerging battle are lack of concern and lack of information about the issue. Many small or rural agencies do not see a need or urgency to address the possibility of breached security because of their size, seeing an attack as only a remote possibility if not a non-existent threat. Consequently, despite simple, inexpensive steps they could take, most are not spending time or money on security. A recent national report showed small and rural government entities spent less than three percent of their IT budget on security.

Clifford Clarke, CIO of the Public Technology Institute, explains, "Personal data tends to be undervalued. Some municipalities don't think they have anything to protect, since the information is considered public." This misperception results in lack of prevention and protection efforts.

**"Personal data tends to be undervalued. Some municipalities don't think they have anything to protect, since the information is considered public."**

**The threat is real, but the solution is simple. Here are several easy, protective measures any municipality or water district can take to greatly reduce their risk of being hacked.**

1. Educate employees about not using computers for personal use.
2. Urge users not to open email attachments from anyone they do not recognize.
3. Install and keep up-to-date anti-virus software.
4. Do not access sensitive data from unsecured mobile devices.
5. Do not plug in USB thumb drives of unknown origin just to see what is on them.
6. If more advanced measures are necessary, contract a third party consultant to assess and recommend solutions.

"Local governments are doing so many transactions online these days, so the risk of a single virus that hits, spreads and shuts down the entire system is real," says Mark Ryckman, city manager for a small city in New York with no IT staff of its own. "We're reliant on these systems, so it's a big impact when they go down."

Kristin Judge, the director of partner engagement at Multi-State Information Sharing and Analysis Center reminds, "Today's hackers aren't kids. They are experienced computer hackers in China or Russia. They can get into your system and they stay in."

On a beneficial note, hackers have been instrumental in the free-flow of information in technological advances. Some of the best programmers were hackers and helped build personal computing as we know and enjoy it. Apple's Steve Jobs for example was a former phreaker. Facebook's Mark Zuckerberg was a hacker, as was Linus Torvalds creator of the Linux system, and Tim Berners-Lee, the man behind the world-wide Web. The Open Source software movement is a direct result of independent-driven people who see a better way of doing things. Ironically and very likely, the free anti-virus program you use to protect yourself from attack was written by hackers. This idea of freedom of speech, freedom of information taken one step off balance is essentially Hactivism, quite simply, Internet civil disobedience.

Perhaps the analogy of hactivism as bacteria fits here. Bacteria is helpful in balance: just wash your hands thoroughly with soap and water.

*Since 1997, Jen Sharp (JenSharp.com) has served business and government across Kansas and the US and even internationally, specializing in Web development, design & programming including e-Learning, ecommerce, content management systems, and other small business solutions.*



**EEI** Earles Engineering & Inspection, Inc.

CIVIL & STRUCTURAL ENGINEERS • SURVEYORS  
CONSTRUCTION INSPECTORS

WOMEN OWNED MINORITY FIRM- DBE CERTIFIED

email: [earlesinc@earleseng.com](mailto:earlesinc@earleseng.com) • Web site: [earlesengineering.com](http://earlesengineering.com)

Liberal: 620-626-8912 • Salina: 785-309-1060 • Garden City: 620-290-4176

*Design of water, sewer, drainage, streets, bridges, wells, pump stations, wastewater treatment, and surveying, construction inspection and testing, including QA/QC*

1-800-327-9761 (except FL)

E-mail: [regal@regalchlorinators.com](mailto:regal@regalchlorinators.com)

TEL (772) 288-4854

FAX (772) 287-3238

**regalchlorinators**  
incorporated

1044 S.E. Dixie Cutoff Road, Stuart, FL 34994 USA  
[www.regalchlorinators.com](http://www.regalchlorinators.com)

**REGAL GAS CHLORINATORS: PURE WATER. PURE AND SIMPLE.**