UNDER ATTACK

CelebrityPress®

UNDER ATTACK

How to Protect Your Business & Your Bank Account From Fast-Growing, Ultra-Motivated and Highly Dangerous CyberCrime Rings

DANIEL FOOTE

With Other Leading Cybersecurity Experts From Around The World

LOCKING OUT CYBERCRIMINALS: THE SOLUTION IS LAYERS, NOT WALLS

Under Attack

"How To Protect Your Bank Account From
Fast-Growing, Ultra-Motivated and
Highly Dangerous CyberCrime Rings"

by Daniel Foote

Celebrity Press™ Publishing

(Excerpt from the chapter, pages 1-2)

You're an original; don't become a statistic by overlooking prevention.

There is no "one-size-fits-all" IT plan for creating a more secure business network.

Every business is different, and has different needs. Compared to small businesses, banks and financial institutions employ complex methods to ensure the highest levels of security available. Hospitals and large healthcare organizations choose different security techniques from what a small clinic might. Regardless of the size of the entity, the approach comes down to one factor: **the ability to allocate resources plus the staffing to monitor the systems necessary to manage all technology that has been implemented**.

Larger businesses aren't invincible, but overall, they're better protected than the smaller businesses that may be under the illusion that they are insignificant. Think of a speck of sand in the desert. *At first glance, you think that it blends in and could never be singled out*. Guess what? **Cybercriminals are experts at finding that speck of sand and exploiting it to a high degree**. Our understanding of this is a large reason why DanTech Services is quite passionate about educating and informing smaller businesses about data protection and intrusion prevention—no exceptions to the rule!

When technology and humans collide . . .

Data security is a partnership between the employees of a business and the technology that has been put into place.

The relationship between a business's employees and its technology is very important. You can have the best technology in place, but if your employees don't understand their role in protecting its integrity, it's incomplete. Likewise, you can train your employees on what to do and not to do with technology in the workplace, but if you don't have excellent security measures in place, your data is still highly vulnerable. Nothing better emphasizes this point than the following situation, which really happened:

> Phil is an IT specialist and he goes to perform a routine audit for one of his clients. He enters the building and is glad to see that everything is as it should be: he has to sign in at the front desk and cannot gain access to anything confidential without the appropriate management's presence. It's ideal, and he's thinking, *this is great, a real success story.* He walks through the building and sees that all suggestions are in place and continues to be more impressed. There's only one check left in the physical security layer, which is the perimeter of the building.
>
> Once outside, Phil walks to a building next door and goes to the roof to assess his client's building from a different angle. This is when things get interesting. He sees a fenced area in back of the building. Inside this 'protected' area, there is a door open that leads inside. There is also a ladder, in the grass, next to the fence. Once the ladder is moved against the fence, anyone who can climb a ladder can now scale the fence. Red flag. Curious as to what he may find, Phil leaves his observation spot and makes his way over to the fence, uses the ladder to go over the fence, and effortlessly walks right into one of the most highly secured areas of his client's business.

What's the moral of this story? The most advanced strategies and systems can be overridden when common sense doesn't prevail. **Never overlook the obvious, because data thieves do not**.