ISS INSIDE SELF-STORAGE

Cyber Scams to Avoid During the Coronavirus Pandemic and Other Times of Crisis

Safeguarding your self-storage business against cyber attacks is always important, but it's even more critical in times of crisis when the criminal element will step up its game. Here's how to practice "virtual hygiene" during the coronavirus pandemic and any other national emergency.

John Iannarelli | Mar 25, 2020

During the novel coronavirus (COVID-19) pandemic, we've all heard the importance of good hygiene: maintain social distance, avoid unnecessary crowds and, above all, wash your hands. These strategies are meant to keep us safe as the virus takes its

somewhat unpredictable course. But to fully protect ourselves during this crisis, we must also practice *cyber* hygiene. This is especially important for businesses like self-storage, which handle sensitive customer information.

Cyber hygiene ensures computers and their users aren't unnecessarily exposed to digital viruses. Malware, ransomware and other nefarious bugs can infect computers and systems, making them "ill," preventing them from operating as they should and hurting us in the process.

Cyber criminals have always used current events to facilitate their wrongdoings. In times of terrorist attack or natural disaster, scams will appear online claiming to raise money for charity or asking you to enter your personally identifiable information. COVID-19 is just another opportunity. While many are hard at work curing the sick and others are simply out of work, cyber criminals are busy spreading their own unique plague. They're leveraging human concerns and fears over this tragedy to steal passwords, data and money.

Scams Under Way

For example, it's estimated that nearly 50 percent of all coronavirus-themed domain registrations are likely to be infected with malware or posted by malicious actors in an effort draw in those seeking information. A site that purports to have suggestions on how to avoid the COVID-19 can trick visitors into downloading malware under the guise of medical guidance. Once a computer is infected, hackers can access all information within, including login credentials and passwords.

Even legitimate websites can pose a danger. For example, a tracking map from a major medical university was recently targeted by hackers. In this scam, website visitors were instructed to download software, which generated a fake map infected with malware, thereby contaminating the user's computer. Fortunately, those working at the university were experts in medicine *and* cyber security. They quickly discovered the resolved the issue.

Phishing scams have also been prominent during COVID-19, with e-mails filling inboxes that appear to be from the Centers for Disease Control and Prevention. These messages lure clicks to links that claim to offer information about the virus but are just another vehicle to inject malware.

Furthermore, while schools are canceling classes, cyber criminals are creating false e-mails to students and teachers, alleging to be from personnel such as the institution's "health team." They're directing computer users to fake login pages that result in the theft of credentials. Further complicating this scam is the fact that users tend to use the same login information across multiple websites, making it easy for criminals to gain unauthorized access in many places.

Most disturbing of all is hackers working on behalf of the Chinese government are capitalizing on the circumstances created by coronavirus to install malware and steal information. North Korea and Russia are also suspected of exploiting the situation, preying on peoples' concerns through phishing attacks. Fortunately, there's often a cure for a computer virus.

Take Action

Like the good physical hygiene we're encouraged to use to avoid COVID-19, we all need to employ sensible cyber hygiene to avoid digital viruses. Here's what you can do to minimize risk:

- Be wary of anything you click. Make sure it's from a reliable source. Better yet, go to the source's Web page and obtain the information directly from the site to avoid any chance of inadvertent contamination.
- Now is definitively *not* the time to download e-mail attachments unnecessarily, even from people you know, as they might be unwittingly passing a malware-infected attachment.
- Keep your antivirus software and other programs current and regularly run a virus scan of your computer.

The coronavirus is doing damage, but eventually the threat will pass. While many will be impacted, life will soon normalize. However, computer viruses are here to stay. The circumstances may change, but the dangers of cyber criminals are always the same. Fortunately, you have the power to protect yourself. Practicing good cyber hygiene so will not only help keep you safe, it'll allow you to focus attention where it really matters—on yourself, your loved ones and your livelihood.

John Iannarelli is an associate of The Safety Institute, a health and safety resource for businesses. A retired FBI agent, he has firsthand knowledge of emergency procedures. He's also a recipient of an honorary Doctor of Computer Science in recognition for his contributions to the field of cyber investigations. For more information, e-mail nona@safetyinstitute.com ; visit www.safetyinstitute.com .