



The Old BARN POST

Quarterly Newsletter of The Hess Agency

Winter 2020

Hacking Without a Cold

Hopefully, you have avoided the bug that seems to be going around this winter. Several people I know have a lingering cough that seems to be hard to get rid of. Even my wife, who faithfully gets her annual flu shot, has had a stubbornly stuffy nose for a couple of weeks now.

While annoying coughs are nothing to sneeze at, a potentially more serious kind of hacking increasingly has been afflicting our customers. Computer hackers seem to be targeting small businesses and others more frequently. I'm told that most of the intruders are based overseas and, with the recent hostilities with Iran and North Korea, we will see even more attempts in the future.

Like the flu virus, these hack attacks come in a variety of strains: Malware, cookie thefts, clickjacking, viruses, passive eavesdropping, and phishing, to name some of the more common ones. Some of these are worse than others, but all involve bad actors seeking to access personal information on your computer.

Our own office computer system was the victim of a ransomware attack a few years ago. One of our farmhands clicked on a seemingly harmless attachment on an email that appeared to come from a customer. It turned out to be a criminal looking to extort money from us by holding one of our computer files for ransom. We were notified that they would release the file back to us if we paid them \$3,500.

After reviewing our options with our IT consultants, we decided not to pay the ransom and instead used our overnight backup to recreate the file. The bad actor did not access our data, they simply prevented us from accessing it ourselves, without the key. In the end, we lost one day's work, which may not sound like a big deal. But if you think about losing 28 people's

productive time for one day, plus the IT time involved to fix the problem, the costs add up quickly. Others have faced much greater losses. High profile cases in the news tell of cities, school districts, and hospital getting hacked, with demands reaching millions of dollars.

While your first line of defense against hackers is to follow best practices to maintain the security of your computer systems, some insurance solutions also can help you tackle tech problems and soften the financial blow if you do get hacked.

For individuals, identity theft protection can be added to a homeowners policy to help cover costs associated with a hacker who steals your personal information.

Cyber insurance can be purchased by businesses to pay for recovering from hacking attacks. The coverage defrays the cost to restore your information, notify anyone required as a result of the breach, and cover litigation that may result from clients' personal information being compromised. Some policies even provide funding for extortion. Many policies provide access to live, expert guidance and assistance throughout the recovery process.

As we begin a New Year, here's hoping that no one steals your cookies or highjacks your clicks in coming months. But if you do get hacked, proper insurance coverage can prevent you from being left out in the cold.

Steven L. Faus, CIC, CLU
President

According to Risk Based Security research, more than 3,800 known data breaches occurred in the first half of 2019, exposing more than four billion records.