VASSEY
Financial Planning & Investments

What We Learned from the WannaCry Ransomware Attack

Presented by Alex Vassey, CFP®

If you've checked the news in the past month, you've likely heard of the WannaCry ransomware attack, one of the most widespread cyber attacks to date. Security experts estimate that more than 200,000 users have been infected with this malware. Once infected, all information on the user's computer is encrypted (i.e., locked away) unless a ransom of $300–$600 is paid to the attackers in Bitcoin.

To make matters worse, there's no evidence that the attackers have ever held up their end of the deal. Generally, when a user pays, the encrypted information is *not* returned in its normal state. In other words, this global attack just leaves the information irrecoverable.

So you might be wondering: What could I possibly do to defend against WannaCry and similar attacks in the future? Let's review four valuable lessons that this recent event has taught us about protecting ourselves.

Lesson #1: Keep up with security news to raise awareness of current threats

Over Easter weekend, a notorious hacker group called the Shadow Brokers leaked confidential National Security Agency (NSA) hacking tools and techniques, including a number of critical Microsoft vulnerabilities. Just a few weeks later, WannaCry struck, taking advantage of one of those vulnerabilities.

If we had all read the news about the NSA leak, we would have been warned that our Microsoft software was wide open to an attack. But even if we had been able to follow these breadcrumbs, what could we have done? That's where Lesson #2 comes in.

Lesson #2: Don't delay your updates

When news of the NSA leak first broke in April, Microsoft immediately stated that it had released an appropriate security patch. In fact, it had released the patch in March—*one month before* the NSA leak. Sounds as if we should've been all set, right?

That would have been true had we all updated our machines on time. Unfortunately, when we're at our computers and an update box appears, we sometimes delay installation because we don't want to be interrupted. But system updates often include critical security patches that protect us from current cyber attacks. Delaying their installation only leaves us vulnerable for a longer period of time.

It turns out that *all* 200,000 victims of the WannaCry ransomware attack had unpatched systems. Though the attack struck in May, these users hadn't updated their Windows operating systems (and subsequently rebooted their computers) since before March, so the patch hadn't taken effect.

The next time you're prompted for an update, keep in mind that it might be the one thing that could protect you from attacks like WannaCry. If you have to delay installation, don't delay for too long.

Lesson #3: If you need that information, back it up

The single most important safeguard against ransomware is backups. If you back up all your important information—and your machine becomes infected with ransomware—you already have a duplicate of everything the attackers are holding for ransom. No need to even consider paying!

But backups are only effective if done right. When adopting a backup process, keep these three tips in mind:

- **Your backup should be stored separately from the system you're backing up.** If you perform local backups on an external hard drive, leave it unplugged from your system when it isn't backing up. If you have a cloud provider, research the protections it has in place to defend against ransomware infections. (Cloud providers typically offer *versioning*, which allows you to roll back to an uninfected version of your files if the files are ever infected or corrupted.)
- **Regularly test your backups.** Imagine believing that you're protected against ransomware—only to be attacked and find that you can't restore your backup properly. It's worth ensuring that the process works. Test a restore from time to time.
- **Secure your backup information as much as you would your original information.** When backing up sensitive information, be sure that it's encrypted and password-protected. If it's a physical hard drive, keep it in a place where no one can easily take it.

Lesson #4: Honor among thieves isn't always a reality

Believe it or not, upon payment, a majority of ransomware attackers actually give users their information back. Unfortunately, in the case of the WannaCry variant, experts believe that the attackers *do not* give the information back—no matter what. So when confronted with WannaCry, we recommend doing as the evidence suggests—don't pay.

If you're hit with any other variant of ransomware, we can't tell you what to do. If you search for answers online, you'll see that some experts recommend never paying. But, ultimately, that decision is up to you. Always research the particular variant for possible alternative solutions, and keep in mind that no one but you can safely say what your information is worth.

Preventing disaster before it's too late

Many of us don't take action until we're part of a major database breach. Yet we should always be preparing for such threats. As we've seen with WannaCry, there were ways its victims could've prevented being affected.

There's no telling what major cyber attack will be in the news next. But if we take the time to find the lessons in the last attack—and apply them to our own lives—we'll be in a much better position to defend our information when the worst happens.

###

Alex Vassey is a CERTIFIED FINANCIAL PLANNER™ professional, a Registered Investment Advisor, and a Chartered Retirement Plans Specialist® with Vassey Financial Planning & Investments, located at 140 Bountyland Road, Seneca, SC 29672. He offers securities and advisory services as a Registered Representative of Commonwealth Financial Network®, Member FINRA / SIPC. Fixed Insurance products and services offered through CES Insurance Agency. He can be reached (864) 718-0600 or alex@vasseyfpi.com. Certified Financial Planner Board of Standards Inc. owns the certification marks CFP®, CERTIFIED FINANCIAL PLANNER™ and CFP *in the U.S.A.*

Authored by Brad McMillan, CFA®, CAIA, MAI, chief investment officer at Commonwealth Financial Network.