VASSEY
Financial Planning & Investments

To Pay or Not to Pay: How to Survive a Ransomware Attack

Presented by Alex Vassey, CFP®

Imagine this: You open an e-mail that seems to come from Google, prompting you to click a link to reset your password. But when you click, a mysterious .exe file downloads and launches. Slowly, all the files on your desktop turn into white paper icons, and the names of all your files turn into scrambled nonsense.

What is happening here? Unfortunately, you've probably fallen victim to a ransomware attack.

The threat defined

Ransomware, as defined by Trend Micro, is "a type of malware that prevents or limits users from accessing their system . . . unless a ransom is paid." Although the term may be new to you, ransomware attacks happen every day. In fact, according to Kaspersky Lab's Securelist, 2.3 million Internet users encountered ransomware between April 2015 and March 2016, and Armada Cloud reports that the volume of attacks grew by 13 percent between August and October 2016.

In the event that a ransomware attack happens to you, it's likely that something much like the scenario mentioned above will unfold. Here's an example of what you might see on your computer screen:

VASSEY
Financial Planning & Investments

Now what?
So, do you pay the ransom or simply wait for the countdown to end? Before deciding, you might try searching online for a free tool that can decrypt your files. But keep in mind that the chances of success are extremely slim. Even if a solution to a previous type of ransomware is available, attackers learn from their mistakes and have likely used a more advanced form of the scheme on you.

You might also consider calling law enforcement. Unfortunately, there's very little that the FBI, for example, can do to resolve an individual ransomware incident. But reporting the crime can help put it on the authorities' radar, so they can work on a solution for future cases.

Most of the time, it all comes down to two choices: either you pay the ransomware fee or you don't.

You pay. One bitcoin equals $778 (at the time of this writing), so paying the ransom may be worth it to you, depending on what those files contain. You hit the Next button and follow the instructions to pay your attacker. What happens now?

- **Outcome 1:** You get your files back. Time to celebrate? Not so fast. From the cyber criminal's perspective, he or she just found a paying customer. Now you're a prime target for another ransomware attack.
- **Outcome 2:** You don't get your files back. Remember: you have no leverage. No one is forcing the criminals to hold up their end of the deal. Even if the attackers are "honorable," you can never be sure that the ransomware will keep your files intact.

You don't pay. Maybe you think the attacker is bluffing. (Hint: If you can't access your files, the attacker isn't bluffing.) Or maybe you've decided that the price tag for your data is too high.

- **Outcome 1:** You're granted a time extension . . . and a price change. Some attackers penalize you for waiting up to their deadline and then not paying. They give you a second chance but increase the ransom. Others realize that you won't take the bait, so they cut you a deal in an attempt to take what they can get. If so, you'll be back to deciding between paying and not paying.
- **Outcome 2:** You don't get your files back. On the bright side, you didn't contribute to one of the worst cyber threats we're facing today. Plus, those attackers won't see you as a receptive victim and may leave you alone in the future.

The best strategy: be prepared!
In the end, it's your decision. It all depends on how much you think your data is worth, as well as how much you trust that the attackers will stick to their end of the bargain. To give you some insight into the choices others are making, a recent Symantec report found that only 3 percent of victims pay the ransom.

Fortunately, there are three relatively simple precautions you can take to prevent such a costly scenario.

1) **Back up your data regularly.** Let's say that you back up your files every Sunday night. If you receive a ransomware threat on—worst-case scenario—a Sunday afternoon, you'll lose only a week's worth of data. If

you would like to start backing up your files, you'll have to take the time to devise your own schedule and method. When establishing a backup plan, remember to keep these two things in mind:

- **Regularly test your backups.** You'd be surprised how many people wait until an attack or hard drive failure before they restore a backup for the first time, only to find that it doesn't work!
- **Store your backups separately from your computer.** If backup media is connected to your system during an attack, your backup data could be targeted as well.

2) Be wary of phishing. Approximately 91 percent of cyber attacks start as phishing scams, according to Wired. When checking e-mail, remember to:

- Hover over all links to verify that they're safe
- Avoid clicking links whenever possible by typing URLs directly into your browser
- Delete any suspicious e-mails

3) Update your systems ASAP. Attackers know the vulnerabilities of yesterday's technology. The longer you avoid regular updates, the more time attackers have to exploit those vulnerabilities.

Most of us haven't experienced ransomware, but as the number of attacks increases, so does the probability of becoming a victim. If the day comes when it does happen to you, will you have a plan for handling the situation?

###

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.