One afternoon last fall, Kevin, an engineer who works for a Florida power company, was quickly checking emails on his home computer when he spotted what he thought was a message containing the mailing label he needed to return some headphones he had recently bought.

The attachment came up blank, so he moved on. Soon his computer began to run a little sluggishly. Then, three hours later, his screensaver—a photo from a South Pacific vacation he and his wife had enjoyed—disappeared. When he checked the directory holding all his photos, he was startled to find them all renamed with strings of gibberish.

Also on his screen was an icon for a document he didn't recognize. He clicked on it and panicked as he read a chilling message: "All of your files are encrypted," it began. And they would be lost to him forever unless he made a ransom payment of $2,400.

"What they had taken was irreplaceable: 20 years' worth of my financial and personal files and every photo taken of my wife and me during the 16 years we've been married," says Kevin, who asked that his last name be withheld to protect his privacy. "The trauma you feel when you understand what's happened to you is overwhelming."

What happened to Kevin and thousands of other people last year could easily happen to you. Your computer or smartphone could be attacked by what's known as ransomware, a fast-growing online scourge that can cost you thousands of dollars if you pay to regain your files—and thousands of dollars if you don't. Also at stake: documents critical to your business or personal finances, priceless family photos, and the days or weeks you might spend trying to replace what you have lost. Want to recover your photos or financial records? You could be ordered to pay anywhere from $200 to $10,000—the range of ransom money typically demanded of individuals, according to a recent IBM Security survey. And nearly a quarter of businesses hit by a ransomware attack end up paying $40,000 or more. As the Department of Homeland Security warned last year, ransomware's effect can be "devastating."

Ransomware has spread with terrifying speed. This type of malware—short for "malicious software"—accounted for fewer than 2% of emails with malicious links or attachments in the fall of 2015, according to PhishMe, a cybersecurity firm. By last fall, ransomware's share had zoomed to a shocking 97%. Total ransomware losses in the U.S. hit $1 billion in 2016, up from $24 million in 2015, the FBI estimated.

More than 5,100 ransomware complaints were reported to the FBI over the past two years. Your odds of being hit, though, are far greater than that figure might suggest; based on an analysis of threats detected by anti-malware programs, the cybersecurity firm Symantec reported ransomware's volume at 4,000 attacks *per day* in early 2016. "Because so many victims never file reports, the cases we know about rep-

PREVIOUS SPREAD: PHOTOGRAPH BY GETTY IMAGES/HERO IMAGES

resent only a very small percentage of what's actually happening," says Will Bales, the supervisory agent in the campaign against ransomware at the FBI's cyber division in New York City.

Just as scary as ransomware's growth is the ease with which you can fall victim to it. This malware, which makes online scams like emails from a Nigerian prince seem almost quaint, can infect your computer not only if you open up a rogue email attachment, as Kevin did, but even if you simply land on a mainstream website booby-trapped by cybercriminals.

What can you do to avoid becoming a victim? Quite a lot, as it turns out. Once you understand the nature of the threat, you can put safeguards into place to minimize the chances of a successful attack. And if, despite your best efforts, your computer is taken hostage, you may be able to recover your files even without paying a ransom. What you need to know:

WHEN RANSOMWARE STRIKES

To be able to take over your computer, cybercriminals first have to get their malware onto your machine. To that end, they're refining other scammers' time-tested stratagems.

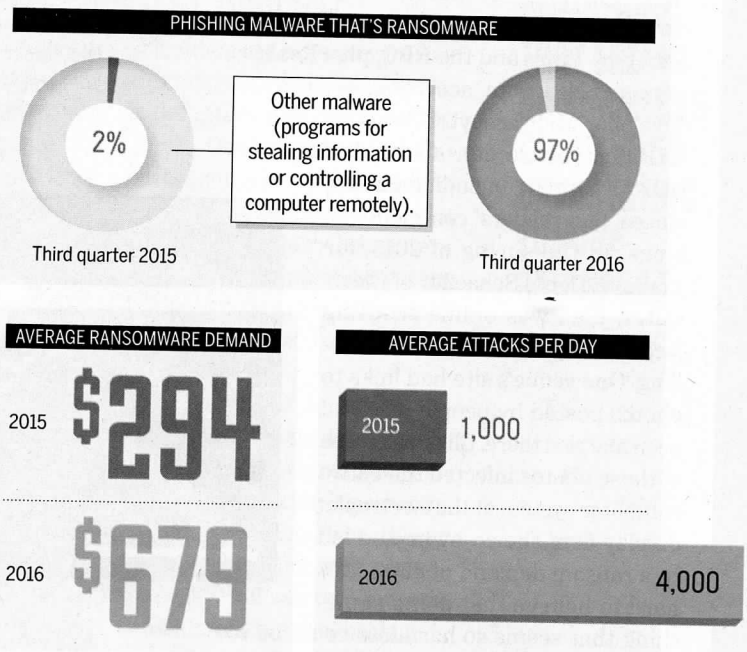
THE SNEAK ATTACK

In the U.S., 59% of ransomware attacks occur via phishing emails that lure you into clicking on malicious links or attachments, according to a 2016 study by Osterman Research. Thanks to a steady stream of data breaches at big names including LinkedIn, Yahoo, and Google, cybercriminals can easily and cheaply obtain a slew of email addresses and other personal information they can use to blast out thousands of ransomware-laden emails, experts say. Then all they have to do is wait for recipients to take the bait.

Though you might think you're a pro at spotting phishes, think again. "Cybercriminals are getting better at creating content that can fool users and bypass detection technologies," reports Osterman.

THE RANSOMWARE EXPLOSION

Incidents of ransomware have grown astronomically, and the amounts demanded are on the upswing too.



NOTE: *Attacks per day in 2016 is for the first three months only.* **SOURCES:** *PhishMe, Symantec*

It was that kind of sophisticated mimicry that tripped up Wolfgang Sailler, a Salem, Ore., financial planner, last September. Sailler had regularly received—and ignored—phishing emails purportedly from banks and other businesses. But an authentic-looking email he received from FedEx about a missed delivery rang no alarm bells, partly because he had recently moved and was waiting for a forwarded FedEx package. So he clicked on the attached delivery notice to get more details. What he got instead was a ransom note demanding $300 to retrieve his encrypted data. "I was angry," he says.

Another delivery mechanism is malvertising—the term for online ads that criminals have covertly embedded with ransomware. Attackers

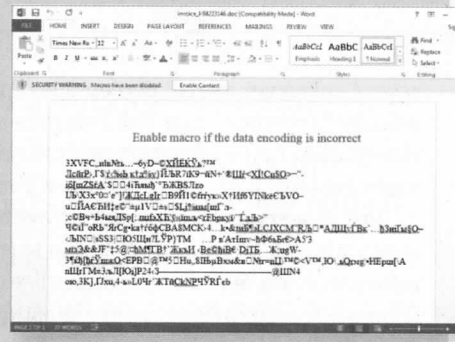
This story is the first in a series looking at the financial risks of digital technology.

THE RANSOMWARE TRAP

Cybercriminals use trickery and fear to separate you from your money.

THE HOOK

You open an attachment or click on a link, and a screen like this pops up, asking you to take some action—in this case, enable a macro in a Microsoft Word document. Do that, and you open the door for ransomware to encrypt your photos and files, turning them into a jumble of characters just as unintelligible as these.



are adept at creating ads that evade detection by the networks that distribute online ads, says John Wilson, chief technical officer at the cybersecurity firm Agari. Even without clicking on those ads, you can be infected just by viewing a web page that carries them. Sites that have unwittingly carried malvertising include those of the *New York Times* and the BBC, plus Realtor .com and NFL.com, according to software developer Malwarebytes.

Ransomware can also hide in other website content, including photos, videos, and readers' comments on blogs. In the spring of 2015, for example, Debbi Schaeffer of Clearwater, Fla., was online scouting locations for her daughter's wedding. One venue's site had links to photos posted by people who had been married there. Clicking on one of those photos infected the entire computer system at the electronic-display firm she co-owns and led to a ransom demand of $500. "It's hard to believe that doing something that seems so harmless could be so devastating to your business," Schaeffer says.

THE SCARE

A ransom note appears, often displaying unsettling images like this vicious clown. The gist: Your photos, files, and other irreplaceable and valuable data will be lost forever unless you follow instructions for paying a ransom. If you cooperate, the attackers promise to send you a private decryption key that will restore your data.

THE PRESSURE MOUNTS

Once on a computer, the malware—either a stand-alone program or code that piggybacks on programs like Microsoft Office and Adobe Flash Player—communicates with the attacker's computer to get encryption keys, which are complicated passcodes it uses to scramble files. The malware targets a wide range of data: files for all types of images, music, documents, spreadsheets, and more.

After the files are encrypted (and perhaps renamed), a process that might take hours, the attackers deliver a ransom note, which either replaces your desktop screen or shows up there as an icon. That note—often accompanied by frightening images of characters from horror movies such as *Saw,*

THE SQUEEZE

To pressure you into paying up, the cybercrooks may set a countdown clock on your screen, ticking off the time remaining until you hit the deadline they have set—commonly 72 hours—to send them the ransom. If you miss their deadline, some ransomware attackers start deleting your files. Others will double the ransom amount that they are demanding.

or Voldemort from the *Harry Potter* series—typically contains a link sending you to a web page with instructions for how to pay the ransom and get your files back. Most impose a deadline of a week or less for you to come up with the ransom, threatening to double the amount or begin deleting your files once the appointed hour passes.

To scare you further, "they'll put a ticking countdown clock on your screen or use other techniques to pressure you to act quickly," says Donn Hoffman, a Los Angeles County deputy district attorney in the cybercrime division. "One variant I've seen covers your locked computer screen with pornographic images."

GETTING DOWN TO BUSINESS

If you decide to pay the ransom, the attackers will go from threatening to extremely helpful, says Ondrej Krehel, CEO of Lifars, a digital forensics and cybersecurity intelligence firm. They want to make it fast and easy for you to pay the ransom, which they usually demand in the form of the digital currency Bitcoin.

"Criminals view this as a business," Krehel says, "and they refer to victims as their clients or customers." In fact, the customer service that some ransomware operators provide rivals that of law-abiding operations, complete with FAQs and online chats with technical support agents who can help you through the process of obtaining Bitcoin and transferring it to them.

Credit the businesslike atmosphere to ransomware's efficiency in generating cash. Unlike identity theft or credit card fraud, which can take months to deliver a payoff, this scam makes money with minimal effort and minuscule risk of being caught. Just one version of ransomware making the rounds in 2016 netted its perpetrators about $34 million from victims paying around $300 to $500 each, according to the information technology company Cisco.

By using Bitcoin and communicating with victims via the anonymizing Internet network known as Tor, criminals who make money from ransomware are difficult to trace, says Leo Taddeo, a former FBI agent now at the cybersecurity company Cryptzone. And even if they are identified, he adds, many of them are based in Russia or some Eastern European countries from which extradition to the U.S. is difficult.

HOW TO PROTECT YOURSELF

As prevalent and insidious as ransomware has become, there are concrete steps you can take to lower your risk of attack and minimize the damage if you're hit. One thing is sure: You can't rely on a particular type of computer to protect you. Although ransomware attacks have primarily targeted Windows computers and Android mobile devices, Apple computers suffered their first ransomware infections in 2016, and iPhones could be next, experts say.

GET YOURSELF SOME BACKUP

A strong backup system for your data is your best safety net, since it will let you restore your hijacked files and photos without paying ransom, says Mark Rasch, a cybersecurity executive at Verizon Enterprise Solutions. For true protection, cybercrime attorney Hoffman recommends having at least two different types of backup.

Start, he says, with an online backup and storage service—one that continuously scans your computer, automatically uploads any new data or changes in existing files, and then stores the most recent version at an offsite data center. Lawrence Abrams, founder of the ransomware information site BleepingComputer.com, recommends using a service that includes "versioning," a feature that allows you to access files older than your most recent backup. Crashplan, Backblaze, and Carbonite are three companies that offer the service, typically charging about $5 a month to cover a single computer.

In addition, regularly back up your data onto a USB drive or an external hard drive, says Hoffman. Even though backup services use tough encryption to protect your stored data, they are not immune to hacking and other digital catastrophes, he says. And be sure to disconnect the

IT'S HARD TO BELIEVE THAT DOING SOMETHING THAT SEEMS SO HARMLESS COULD BE SO DEVASTATING TO YOUR BUSINESS."

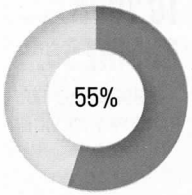
—DEBBI SCHAEFFER, RANSOMWARE VICTIM

SCREEN IMAGES COURTESY OF BLEEPINGCOMPUTER.COM

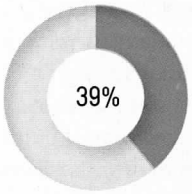
PARENTS WILL GIVE IN

Having children makes you more willing to fork over cash for your files.

PEOPLE WHO'D PAY FOR PHOTO RECOVERY



Parents



Nonparents

SOURCE: IBM X-Force

drive right after backing up. If it's still plugged into your computer when ransomware hits, the copy you made will be hijacked too.

Depending on the value of your files and how often you add or update them, do your home backup monthly or even weekly. The importance of frequent backups became apparent to Debbi Schaeffer and her partner, James Ullery, after their business was attacked. "The backup we had was 30 days old, so it was missing a lot of critical data that was worth more to us than the $500 ransom they were demanding," says Ullery. "We'd already lost three business days trying to climb out of this mess, so we decided to pay." He and Schaeffer got their decryption key within an hour, but the restoration process, which changed the "last modified" dates of all their files, created organizational headaches. They now do weekly backups of their data onto an external hard drive, which they store offsite as an extra precaution in case of fire or flooding.

STAY CURRENT

Keeping your computer's operating system and other programs up to date is crucial because malvertising and other booby-trapped content tend to prey on vulnerabilities in older software that have been subsequently fixed, says Chester Wisniewski, principal research scientist at the IT security company Sophos. Common targets are operating systems, browsers, and browser plug-ins such as Adobe Reader, Flash Player, and Java. When you get notices that updates and security patches are available, don't ignore them, says Wisniewski. "When people say that they're still using Microsoft Word 2003 because they don't need any new features, they don't understand that it's like driving a car without seatbelts or antilock brakes."

Fortunately, online tools can do most of the updates for you automatically. If your home computer is a Windows PC, download Flexera's Personal Software Inspector, a free security scanner that identifies any programs that need security updates and installs them—in most cases without any effort on your part.

Mac users can also automate the process of finding and installing available updates. Simply open the Apple menu in the top left corner of your screen, select System Preferences, and then click on the App Store option. Click on the heading "Automatically check for updates," where you can turn on this feature.

INOCULATE AGAINST VIRUSES

Installing antivirus software is another good layer of protection, since developers adjust their products to detect ransomware variants soon after they emerge. Two choices of experts are Malwarebytes and Sophos Home, both of which have free versions for PCs and Macs.

The antivirus fight never ends because malware developers regularly update their own software to avoid detection. For example, Cerber, one of the most widespread ransomware families, first appeared in February 2016. Within just nine months, its developers had already released Cerber 5.0, according to Bryan Campbell, a threat intelligence analyst at the technology company Fujitsu.

HANDLE EMAIL WITH CARE

You have probably learned to be suspicious of emails peppered with misspellings and grammatical errors, but criminals are getting better at designing phishing emails without such red flags. No matter how authentic they look, don't click links inside unsolicited emails that appear to come from businesses, your bank, or even the IRS. Instead, call or email using separate contact information you have for the sender to confirm that what you received is legitimate.

If you receive an emailed attachment or link that seems out of character from a friend or relative, call—don't email—to make sure that person really sent it. Agari's John Wilson explains that his mother once received a suspicious email from her choir director, so she emailed him to check before she clicked on the attachment. "But it was the person who'd hacked his email who replied," says Wilson, "so she got a flood of malware as a result."

MORE SCAMS TO WATCH OUT FOR

Ransomware isn't the only form of cyberattack threatening your money and your digital life. Protect yourself from these additional online menaces targeting your technology:

MOBILE MALWARE

A growing amount of malicious software has been designed specifically to attack your smartphone—not just ransomware, but also programs devised to steal usernames and passwords for your financial accounts. That's particularly worrisome, since nearly 40% of people say they interact with their bank primarily via mobile devices, reports Clarabridge, a software firm. Viruses can get delivered not only via email, but also by text messages, games, and other apps.

YOUR DEFENSE: To cut your risks, delete apps you don't use anymore and keep the ones you do use up to date. Install apps only from major stores, such as Google Play for Android devices and the App Store for iOS users, advises Jon Clay of the cybersecurity firm Trend Micro. Avoid third-party app stores, which he says are much more likely to carry counterfeit apps, and ignore emails and text messages inviting you to install an app by clicking on a link.

THE GMAIL PHISH

Even security-conscious techies have fallen for this one. It starts with an email in your Gmail account, apparently from someone you know, containing a believable-looking attachment. Click on it, and you're prompted to sign in again on a normal-looking Google log-in page.

That page, however, is a fake designed to steal your username and password. Once you sign in, a cyberattacker can immediately access everything in your Gmail account. Using "Lost Your Password?" services on other sites—the ones that send you an email to verify it's really you—they can then hijack your accounts at financial institutions and online stores. (And using your previous emails as a model, they can hit your contacts with the same scam.) Google says it's aware of the issue and is working to strengthen safeguards against the problem.

YOUR DEFENSE: Google recommends establishing what's known as two-factor authentication in your Google account settings. This will require you to enter a special passcode anytime you log in from a new machine—a requirement that prevents cybercrooks from seeing your Gmail even if they've stolen your password.

BOGUS HELP

Scammers have long offered fake computer technical support. The latest version starts old-school, with a telephone call. Someone claiming to be from Microsoft tech support calls to alert you to a virus or another urgent problem with your PC. These techies seem credible: By using publicly available directories or information exposed in data breaches, they may know your name and might even correctly guess which operating system is on your computer, says the Federal Trade Commission.

To get at your money, they trick you into installing malware that either steals your information or allows them to remotely control your computer. Then they'll charge you for fixing the security problem they just created.

YOUR DEFENSE: Just hang up. "Microsoft will never proactively reach out to you to provide unsolicited PC or technical support," the company says. "Any communication we have with you must be initiated by you."

Be especially wary of any unsolicited email that instructs you to enable macros to view the content of an attached Microsoft Office document, Wilson adds; it's probably ransomware. Macros are computing shortcuts that automate repetitive tasks—such as inserting your company's name and address in a letter—in programs such as Word. But cybercriminals can create macros that actually contain malicious code instead of useful shortcuts.

WHEN YOU'VE BEEN HIT

If your files get scrambled by ransomware and your data isn't backed up, you face a difficult choice: Pay up, or not? But forking over money isn't your only option for recovering your files.

FIND A KEY

To unlock files encrypted by ransomware, you need what's known as a decryption key—a string of data that, when used by a decryption program, can restore your files to normal.

Your cyberattacker wants you to pay for that key, of course. But cybersecurity researchers and other volunteers have at times cracked code to obtain ransomware keys, which they make available for free. You can find out what type of ransomware you have been hit with and whether a decryption key is available at NoMoreRansom.com, a free website backed by law-enforcement agencies in 25 countries.

Another useful site is Abrams's BleepingComputer.com, where computer forensics experts inform and assist ransomware victims. They have figured out encryption codes themselves for many common families of ransomware, and they link to other reliable sites offering free decryption tools for versions they haven't cracked. BleepingComputer also operates forums where victims can share information to help one another. Robert Orsello,

"CRIMINALS VIEW THIS AS A BUSINESS. AND THEY REFER TO VICTIMS AS THEIR CLIENTS OR CUSTOMERS."

—ONDREJ KREHEL, CYBERSECURITY EXPERT

IF YOU EXPLAIN THAT YOU CAN'T AFFORD WHAT THEY'RE ASKING, THESE PEOPLE WILL NEGOTIATE."

—LAWRENCE ABRAMS, RANSOMWARE EXPERT

a Scottsdale engineer, regained access to his hijacked files in the fall of 2015 with the help of a volunteer. He now donates the use of a high-performance server to help BleepingComputer's engineers crack codes for other victims.

Treat with caution other sites promising help, says Avivah Litan, a cybersecurity analyst at Gartner, an IT research firm. Some criminals lure victims by falsely advertising themselves as ransomware experts while loading computers with even more malware.

PAY THE PRICE...

If you can't get assistance from these Good Samaritans, you might decide to hand over the ransom to retrieve your hijacked data.

Before you pay, Abrams recommends using the customer support links provided in your ransom note to try to negotiate better terms. "We've found that if you explain that you can't afford what they're asking, these people will negotiate because they just want to get paid and move on," he says. In fact, the European cybersecurity firm F-Secure reported recently that three out of four criminal gangs they evaluated were willing to negotiate their ransom fees downward, giving victims an average break of nearly 30% in the cases they examined. And all of them were willing to extend payment deadlines as well.

As for whether you'll get your data back, cyberattackers usually do provide decryption keys in return for ransom, because if they don't, word gets out and fewer victims will pay up. "Last summer a strain of ransomware started going around that deleted people's files even when they'd paid," says Sophos's Wisniewski. "But the guys behind it started getting death threats from other ransomware groups because what they were doing would screw up the scam for the rest of them."

...OR STAND FIRM

If on principle or for economic reasons you choose not to pay, you might want to save your encrypted data; a free decryption key for the ransomware that hit you might become available someday. In that case, Abrams recommends copying your entire hard drive—including all encrypted files and ransom notes—onto an external hard drive. A local computer technician can help you with this process (known as cloning) and also with clearing malware and encrypted files off your computer's infected hard drive so that you can get back to using it. Then periodically check online to see if decryption tools for your strain of ransomware are available yet.

That's what Kevin, the Florida engineer, ultimately did. "I have the resources to pay the $2,400 ransom, but I refuse to give these criminals money to become even more proficient at ruining the lives of other people," he says. "It's only a matter of time until a free decryption key becomes available, so I'm going to let my files and photos stay safely frozen in time off-line until that day comes."

Sailler, the financial planner, also chose not to pay. "I keep all of my crucial business or personal information on a computer that is never connected to the Internet," he says. He simply wiped his hard drive clean.

Whether you pay ransom or not, report the attack to the FBI at IC3.gov, as Kevin did. Last fall the agency urged victims to file reports to help it get a better picture of ransomware's spread and impact. When Kevin returned to work after his ransomware attack, he learned something about the scope of the threat. "In just the first few days I was back, several people told me that the same thing had recently happened to them or someone they were close to," he says. "If they hadn't overheard me talking about my own experience, they never would have mentioned theirs, which says something to me about how big this problem really is." M

MORE ONLINE

Watch a ransomware expert explain more about the spread of malware and how to defend yourself against it at **money.com/video.**

HAVE YOU BEEN HIT BY RANSOMWARE? *Tell us at letters@moneymail.com.*