Ransomware: When the Criminal Locks the Filing Cabinet

Imagine turning on your computer one morning and discovering that your photographs, tax records, financial files, correspondence and other important documents are still there—but you can't open any of them. Then a message appears announcing that your files have been encrypted. If you want them back, you'll have to pay.

Welcome to **ransomware**, one of cybercrime's most profitable inventions. Unlike malware that quietly spies on you or steals information without your knowledge, ransomware wants your attention. Its purpose is essentially the same as kidnapping: take something valuable away from the victim and demand money for its return.

The good news for home computer users is that ransomware isn't invincible. Sensible precautions can make an attack less likely, and good backups can take away much of the criminal's leverage.

The Hospital That Went Back to Paper

One of the stories that prompted me to write about cybersecurity years ago occurred in February 2016 at Hollywood Presbyterian Medical Center in Los Angeles. A ransomware attack disrupted the hospital's computer network and prevented employees from accessing important computer systems.

The hospital found itself dealing with a very modern emergency by resorting to decidedly old-fashioned technology. Some computer-dependent activities were disrupted, and employees relied on paper and other workarounds while technicians tried to restore normal operations. After days of disruption, the hospital paid approximately $17,000 in Bitcoin to obtain a decryption key.

The incident attracted national attention partly because it demonstrated that ransomware could affect much more than somebody's home computer. Hospitals, businesses, schools, government

agencies and other organizations had become attractive targets. Nearly a decade later, ransomware remains a serious threat.

What Ransomware Actually Does

Traditional ransomware generally works by denying access to a computer or its information. Early **locker ransomware** could prevent users from operating their computers while leaving the underlying files largely intact. The screen might display an alarming notice claiming that law enforcement had detected illegal activity and demanding payment to restore access.

More dangerous **crypto ransomware** encrypts files themselves. Encryption ordinarily protects information by converting it into an unreadable form that can be restored with the proper key. Ransomware turns that valuable security technology against the victim. The criminal encrypts the files and controls the key needed to restore them.

Modern ransomware attacks can go a step further. Criminals may steal information before encrypting it and threaten to release confidential material if the victim refuses to pay. For businesses and organizations, the threat may therefore involve both losing access to information and having stolen information exposed.

How Does It Get Into the Computer?

There isn't a single ransomware entrance. Criminals can exploit unpatched software, compromised accounts and poorly protected remote-access systems. For ordinary computer users, however, familiar social-engineering tricks remain important.

An unexpected email attachment may contain malware. A fraudulent message may lead to a malicious website. Bogus software or a fake update may persuade someone to install something that shouldn't be there. A stolen password can sometimes give an attacker access without requiring the victim to download anything at all.

That is why the precautions discussed throughout this cybersecurity series overlap. Keeping software updated, being cautious with email, using strong and unique passwords and enabling multifactor authentication don't merely protect against one particular threat. Together they close several possible doors.

Why Not Just Pay the Ransom?

Faced with the loss of irreplaceable files, paying may seem like the obvious solution. Unfortunately, you're negotiating with criminals, not a reputable computer-repair company. Paying doesn't guarantee that a working decryption key will arrive, that all the files can be recovered, or that stolen information will actually be destroyed.

Payment also demonstrates that ransomware can be profitable. Law-enforcement agencies therefore discourage paying ransoms, although organizations facing an actual attack may have complicated legal, financial and operational decisions to make.

For the home user, a better strategy is to reduce the criminal's bargaining power before an attack ever occurs.

The Backup Is Your Escape Hatch

Suppose a ransomware criminal encrypts the only copy of a manuscript you've spent three years writing. The criminal has considerable leverage. Now suppose the same manuscript also exists on a backup that the ransomware cannot reach. The attack is still a serious nuisance, but the criminal has lost the most important weapon: your desperation.

Important files should therefore exist in more than one place. Family photographs, tax documents, financial information, writing projects and other irreplaceable material deserve regular backups.

Cloud storage can provide useful protection, particularly when the service retains previous versions of changed files. But an additional backup that isn't continuously connected to the computer provides another layer of protection. An external drive used for backup can be disconnected when it isn't needed, placing it beyond the reach of malware running on the computer.

And a backup shouldn't merely exist. Occasionally make sure you can actually restore something from it. Discovering that your backup hasn't worked for six months is considerably better on an ordinary Tuesday afternoon than after ransomware has encrypted the originals.

Keep Your Defenses Boring

Effective cybersecurity isn't particularly dramatic. Keep the operating system and applications updated. Be wary of unexpected attachments and downloads. Use unique passwords and multifactor authentication. Maintain good backups. Don't give strangers remote access to your computer.

None of these precautions would make an exciting Hollywood thriller, but that's exactly the point. Good cybersecurity should be boring. The objective isn't to defeat a hooded hacker in an electronic duel. It's to make your computer an unattractive and unrewarding target.

Take Away the Criminal's Power

Ransomware succeeds because our digital possessions matter. Photographs may represent decades of family history. A writer's computer may contain years of work. Financial and tax records can be difficult or impossible to reconstruct. The criminal doesn't have to understand why a particular file matters. He merely has to prevent you from reaching it.

That's why the humble backup is such a powerful cybersecurity tool. It changes the conversation from *Pay me or you'll never see your files again* to *This is going to be an aggravating afternoon.*

Given a choice between those two outcomes, I'll take the aggravating afternoon every time.