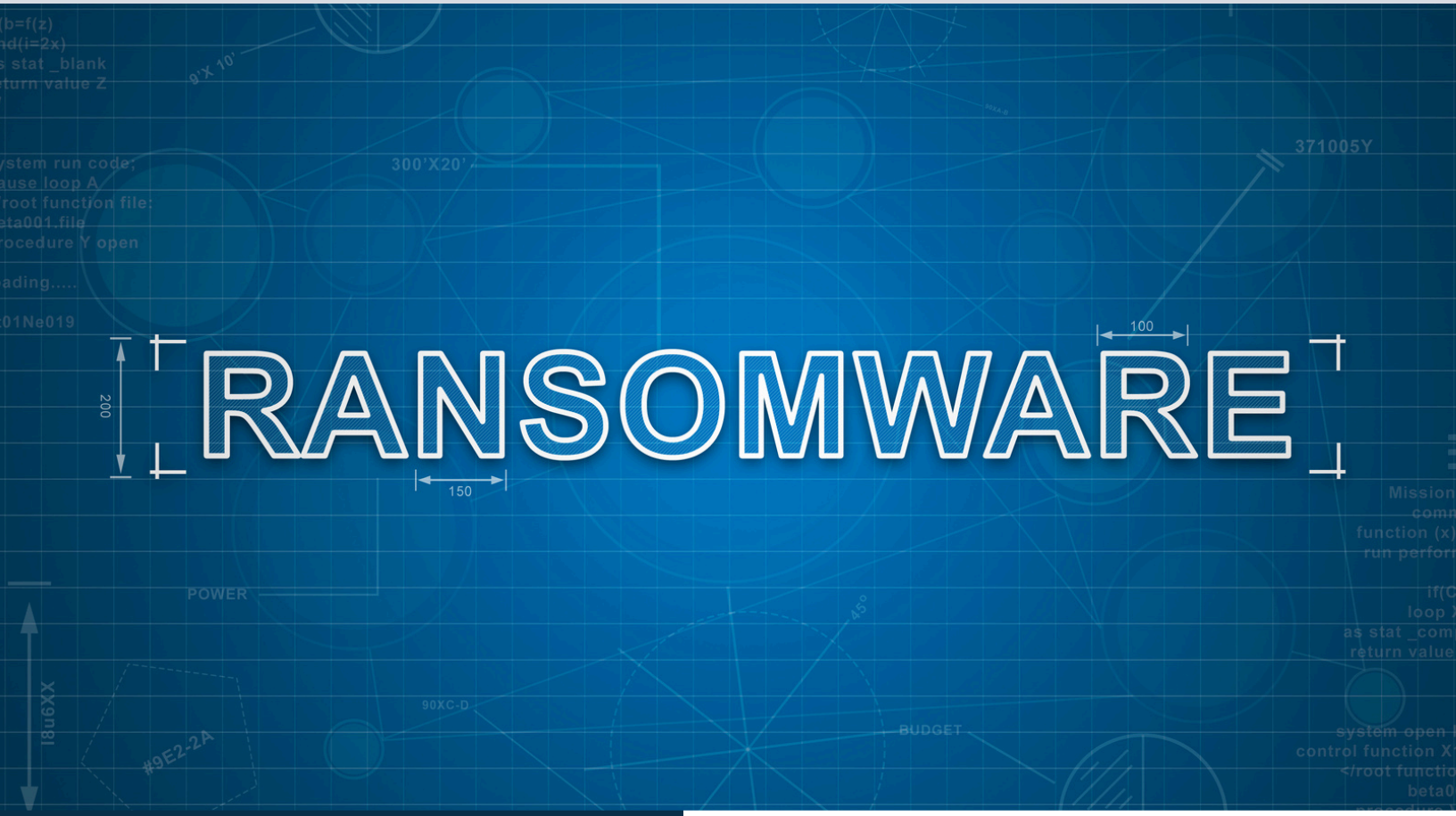
RANSOMWARE: UNDERSTANDING THE THREAT BEFORE IT STRIKES

Lessons from the past, and protections for the future



THIS MONTH'S TOPICS:

Ransomware has become one of the most disruptive cyber threats facing organizations of every size. While headlines often focus on multimillion-dollar ransom demands, the real damage extends far beyond the payment itself.

In this month's newsletter, we'll look back at some of history's most significant ransomware attacks, uncover the hidden costs organizations face after an incident, and explore practical steps every employee can take to help reduce ransomware risk. By understanding how these attacks happen, we can all play a role in making our workplaces more resilient.

Ransomware Attacks That Changed Cybersecurity

Ransomware isn't a new threat, but over the last decade, several major attacks have changed how businesses think about cybersecurity. These incidents demonstrated that ransomware can disrupt hospitals, pipelines, schools, governments, and global companies in just a matter of hours.

WannaCry (2017)

A vulnerability in older Windows systems allowed WannaCry to spread rapidly across more than 150 countries. Hospitals canceled appointments, businesses shut down operations, and more than 200,000 computers were infected worldwide.

NotPetya (2017)

Initially disguised as ransomware, NotPetya was actually designed to permanently destroy data. The attack disrupted global shipping, manufacturing, and pharmaceutical companies, causing an estimated $10 billion in damages worldwide.

Colonial Pipeline (2021)

A ransomware attack forced Colonial Pipeline to temporarily shut down fuel deliveries across the East Coast, leading to widespread fuel shortages and demonstrating how cyberattacks can disrupt critical infrastructure.

MGM Resorts (2023)

Attackers used social engineering to trick the IT help desk into resetting employee credentials. The attack disrupted hotel operations, digital room keys, reservation systems, and casino services, resulting in approximately $100 million in financial losses.

Change Healthcare (2024)

One of the largest healthcare cyberattacks in U.S. history disrupted insurance claims, pharmacy services, and patient care nationwide, demonstrating how ransomware can directly affect healthcare delivery.

HIDDEN COSTS OF RANSOMWARE

When ransomware makes the news, the ransom payment usually grabs the headlines. However, many organizations discover that the ransom itself represents only a fraction of the total cost.

1

Business Downtime

Employees may be unable to access files, systems, or applications for days—or even weeks.

2

Lost Productivity

Teams often return to manual processes while systems are restored.

3

Recovery Expenses

IT teams must rebuild systems, investigate the attack, restore backups, and strengthen security.

4

Legal & Regulatory Costs

Organizations may need to notify customers, investigate potential data breaches, and meet legal reporting requirements.

5

Reputation Damage

Customers and business partners may lose confidence after an attack, affecting future business opportunities.

6

Employee Stress

Cyber incidents create uncertainty, longer workdays, and added pressure on staff throughout the recovery process.

Most ransomware attacks don't begin with sophisticated hacking. They begin with everyday mistakes that attackers know how to exploit.

ACTIONS TO REDUCE RISK

PAUSE BEFORE CLICKING UNEXPECTED LINKS OR ATTACHMENTS

VERIFY UNUSUAL REQUESTS THROUGH ANOTHER COMMUNICATION METHOD

KEEP SOFTWARE UPDATED WHENEVER UPDATES ARE AVAILABLE

USE STRONG, UNIQUE PASSWORDS AND ENABLE MULTI-FACTOR AUTHENTICATION

SAVE IMPORTANT WORK TO APPROVED COMPANY STORAGE LOCATIONS SO BACKUPS REMAIN AVAILABLE

REPORT SUSPICIOUS EMAILS OR ACTIVITY IMMEDIATELY, EVEN IF YOU'RE UNSURE

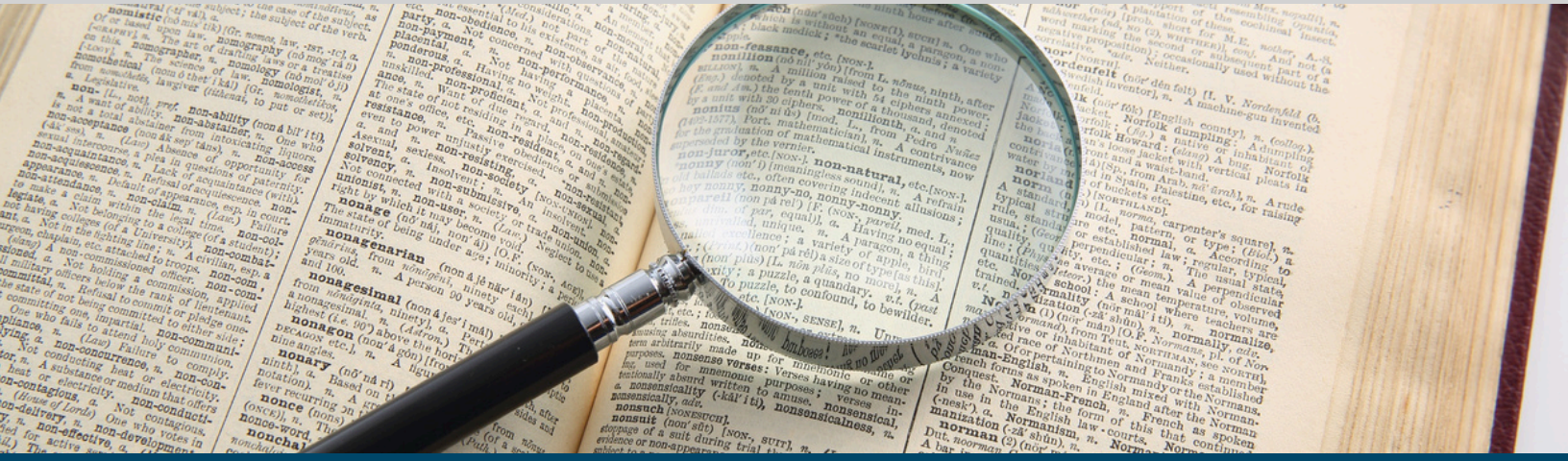
Remember, cybersecurity isn't only an IT responsibility. Every employee who recognizes suspicious activity, follows company policies, and reports concerns helps strengthen the organization's defenses against ransomware.

SCAM OF THE MONTH: DICTIONARY ATTACKS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

When Emily arrived at work on Monday morning, she was surprised to find herself locked out of several company accounts. IT quickly discovered that someone had successfully logged in using her password: Summer2025! Emily hadn't clicked on a phishing email or downloaded any suspicious files. Instead, attackers had used an automated tool that rapidly tested thousands of common words, names, and predictable password combinations until they found the right one.

Because Emily had reused that same password across multiple work applications, the attackers were able to access several systems before the account was secured. Fortunately, multi-factor authentication stopped them from causing even more damage. The incident served as a reminder that simple, easy-to-guess passwords, even with numbers or symbols added, can still be vulnerable to dictionary attacks, where cybercriminals systematically try common words and familiar password patterns until one works.



DID YOU SPOT THE RED FLAGS?

- The password was based on a common word and a predictable pattern.
- The same password was reused across multiple accounts.

HOW TO PROTECT YOURSELF

- Create long, unique passphrases instead of simple dictionary words (for example, River!Coffee7Moon).
- Enable multi-factor authentication (MFA) wherever possible to add an extra layer of protection.