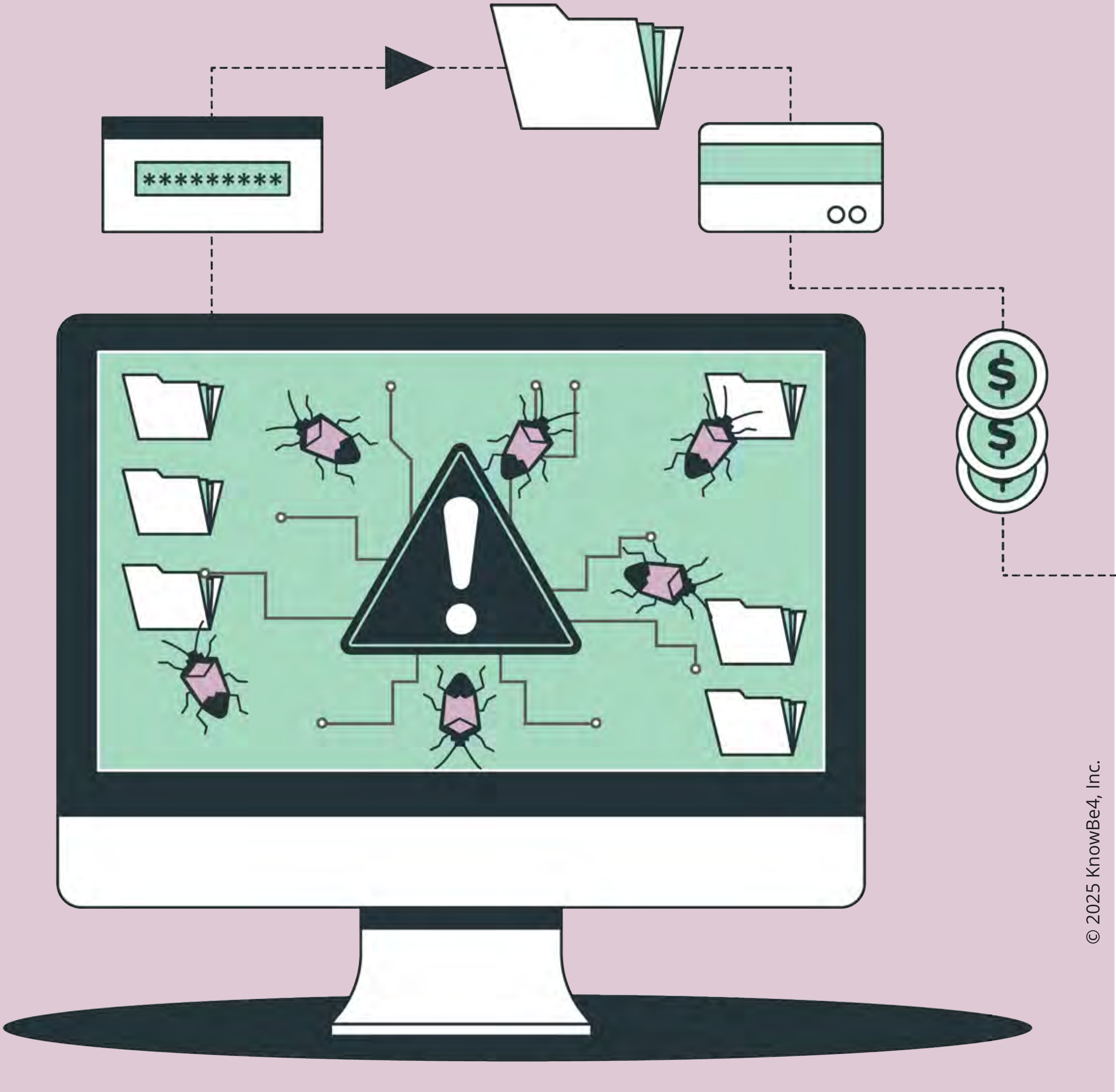
Security Awareness News

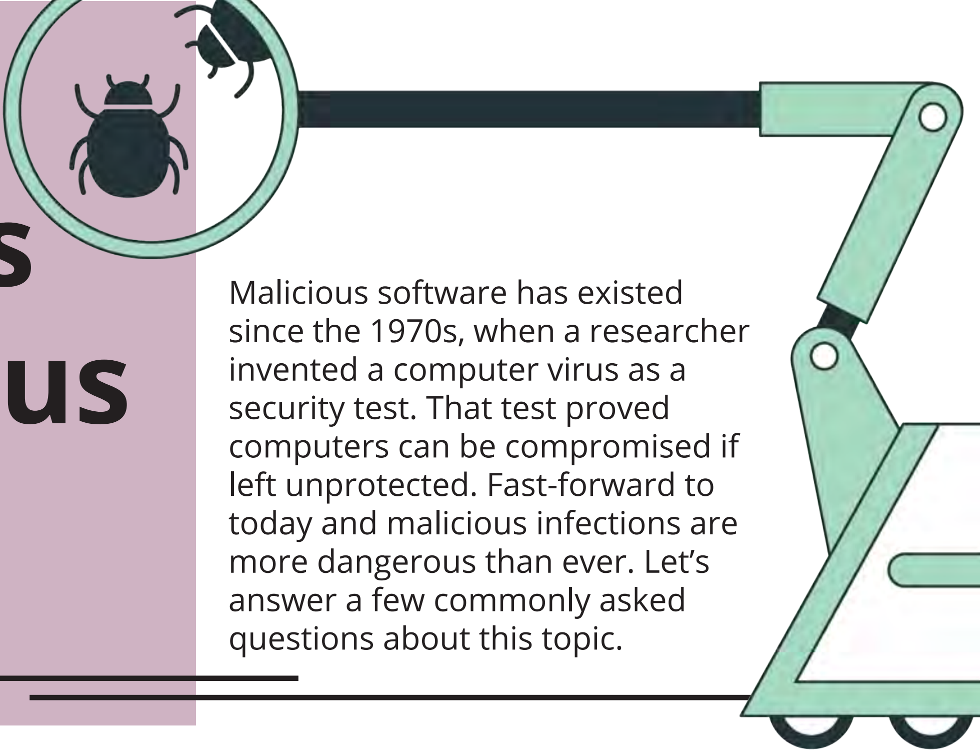
the security awareness newsletter for security aware people

The Dangers of Malware

The Basics of Malicious Software
How Devices Get Infected
Ransomware Case Study



The Basics of Malicious Software



Malicious software has existed since the 1970s, when a researcher invented a computer virus as a security test. That test proved computers can be compromised if left unprotected. Fast-forward to today and malicious infections are more dangerous than ever. Let's answer a few commonly asked questions about this topic.

What is malware?

Malware stands for malicious software — the umbrella term covering any form of malicious code that alters the functionality of computers and smart devices. Attackers use many different types of malware for various purposes.

What can malware do?

It all depends on the attacker's intentions, but generally, malware can be used to:

- Spy on people
- Steal confidential information
- Encrypt data or lock systems
- Corrupt computers and mobile devices

Where does malware come from?

Malware is typically created by criminal hackers who are versed in application development. It can also be purchased or rented by other cybercriminals who don't have the resources or knowledge to develop malware themselves, a process called malware-as-a-service.

How does malware spread?

There are many ways to infect devices with malware, the most common of which is phishing. Phishing refers to attacks that attempt to lure people into making security mistakes. These attacks often feature malicious links or attachments that can spread malware or steal information.

What is the most dangerous type of malware?

They all carry levels of risk, but ransomware is of particular concern. It encrypts data or locks systems, blocking access to critical resources. This can lead to major financial losses, disruption of services, and even threaten lives when it impacts hospitals.

How do you avoid malware infections?

Given that phishing attacks are the most common way malware infections occur, it's the one you should remain the most prepared for. You can identify phishing attacks by staying alert for common warning signs, such as threatening language, urgent requests, and unrealistic promises.

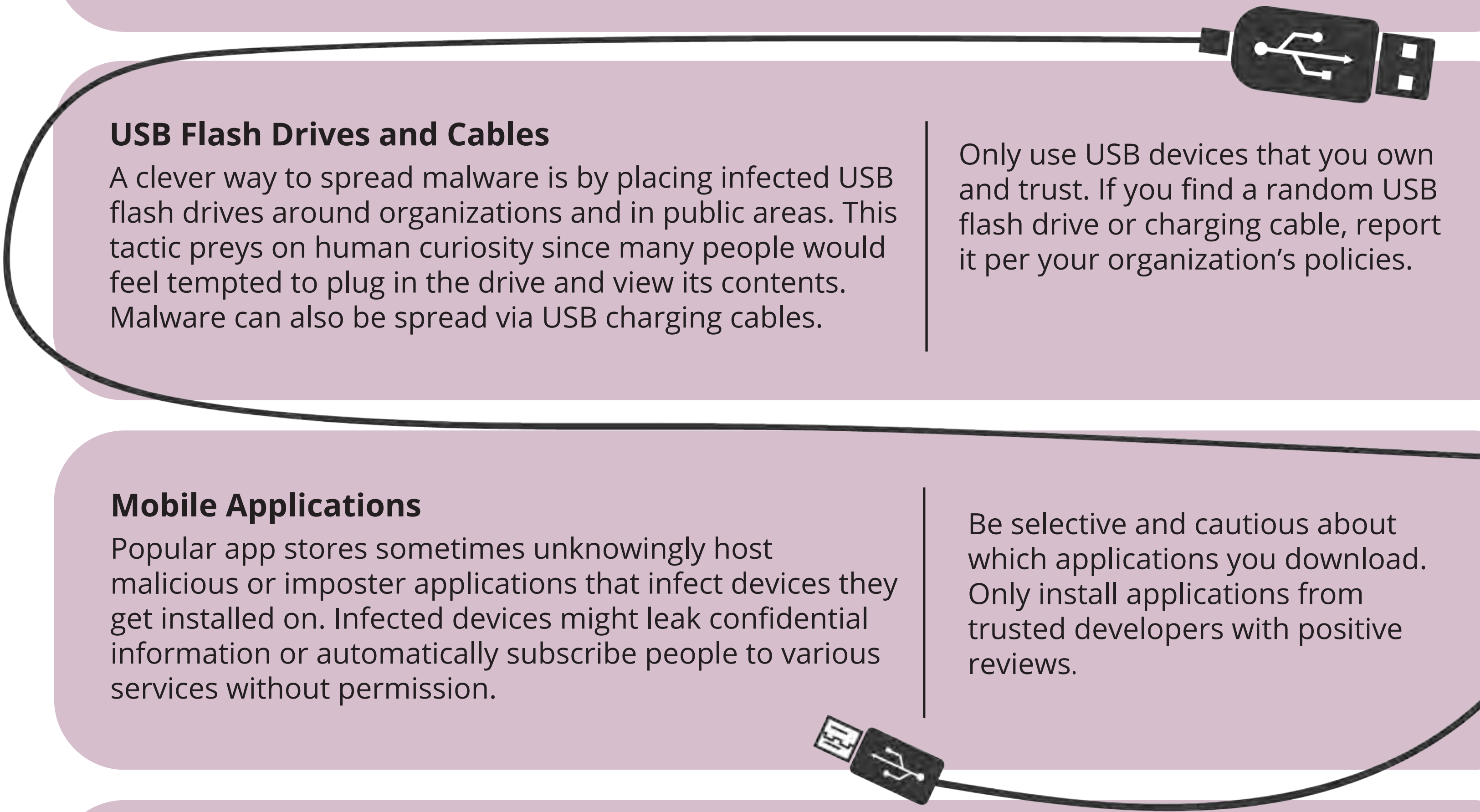
How Devices Get Infected

We've established that phishing is the top threat and is frequently used by criminals to spread malware. It's, of course, not the only threat. Here are a few other ways malware finds its way onto computers and mobile devices.

Outdated Software and Firmware

Unpatched, outdated software and firmware leaves doors open for cybercriminals to exploit vulnerabilities and infect devices with malware. Developers release frequent security updates to close those doors. Failure to install updates in a timely manner invites unnecessary risk.

At work, always follow policies for when to update software and firmware. At home, consider enabling automatic updates so you never miss an important security patch.



USB Flash Drives and Cables

A clever way to spread malware is by placing infected USB flash drives around organizations and in public areas. This tactic preys on human curiosity since many people would feel tempted to plug in the drive and view its contents. Malware can also be spread via USB charging cables.

Only use USB devices that you own and trust. If you find a random USB flash drive or charging cable, report it per your organization's policies.

Mobile Applications

Popular app stores sometimes unknowingly host malicious or imposter applications that infect devices they get installed on. Infected devices might leak confidential information or automatically subscribe people to various services without permission.

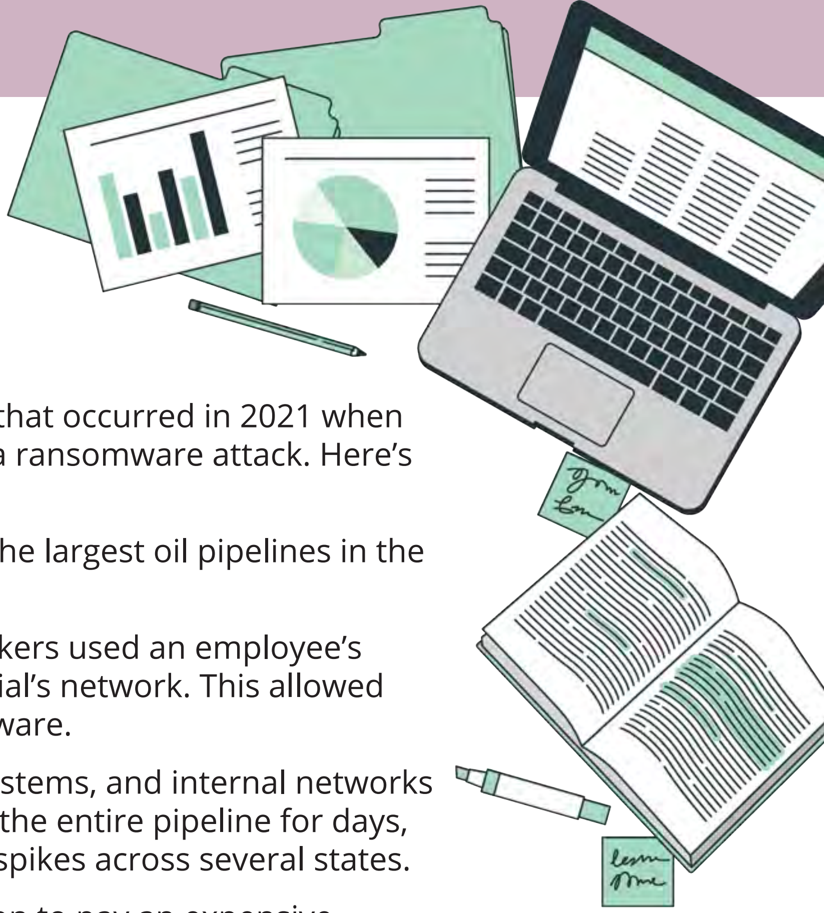
Be selective and cautious about which applications you download. Only install applications from trusted developers with positive reviews.

Malicious Advertisements

Adware is a common type of malware that displays unwanted advertisements and can cause device performance issues. Some of those advertisements may contain other forms of malware that, when opened, infect the user's device.

On personal computers, protect your web browser with adblocker plugins, which can block or limit various advertisements while you browse the internet.

Ransomware Case Study



The following case study examines a real event that occurred in 2021 when an American oil pipeline company fell victim to a ransomware attack. Here's what happened:

Target: The Colonial Pipeline, which is one of the largest oil pipelines in the United States.

Attack Vector: Researchers believe the attackers used an employee's compromised password to gain access to Colonial's network. This allowed them to steal data and then deploy the ransomware.

Impact: The attack made computers, billing systems, and internal networks inaccessible. This caused Colonial to shut down the entire pipeline for days, leading to widespread fuel shortages and price spikes across several states.

Resolution: Colonial made the difficult decision to pay an expensive ransom fee so they could restore their systems.

Lessons Learned:

This attack showcases that ransomware harms more than just the hacked organization. It impacted millions of people and became a national emergency. It was also made possible by a lapse in one of the most basic concepts of security: password management.

The attackers used a stolen password to gain access to Colonial's network. That password was likely obtained as a result of an entirely different security breach. This means the password was likely used for more than one account.

It also means there was no multi-factor authentication (MFA) in place. MFA requires two or more forms of authentication before access is granted. Even though the attackers had the correct password, they would have been much less likely to have access to additional authentication factors had MFA been implemented.

Key Takeaways

- Use strong, unique passwords for every account. A strong, unique password is long, hard to guess, and adheres to organizational policy.
- Implement MFA. This tool adds an extra layer of security by requiring multiple forms of authentication.
- Stay alert for phishing scams. Phishing is how passwords are sometimes stolen and is the most common way ransomware spreads.