

# HOW DOES A RANSOMWARE INFECT YOUR COMPUTER? & WHAT YOU CAN DO TO STAY SAFE.

## RANSOMWARE

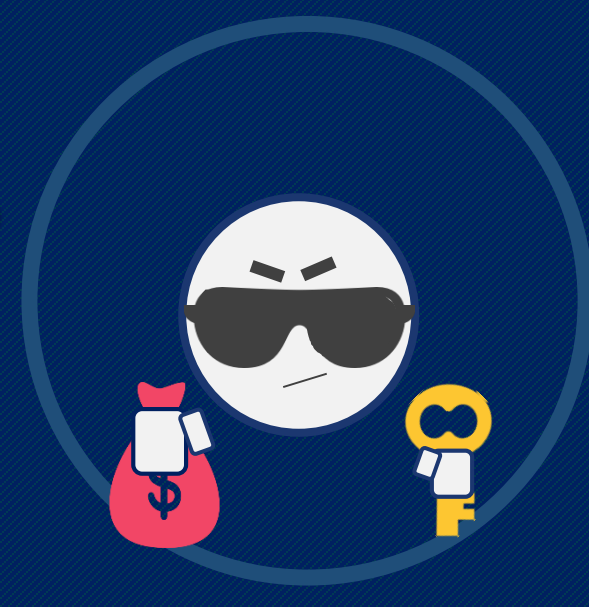
is the **5th** most common form of malware in 2017.

Verizon Data Breach Investigation Report 2017

a malicious software that locks your computer or encrypts your data and demands a ransom in exchange and thus the name 'ransomware' = ransom + malware

Money demanded in some of the recent ransomware attacks of 2017 ranged from 79\$ to 4000\$ (mostly in Bitcoins)

## THE 2 MOST COMMON CHANNELS ransomware use to infiltrate your computer



# #1. EMAIL

Emails serve as the most resourceful tool to deliver ransomware.

“93% of all phishing emails contained encryption ransomware in 2016.”

PhishMe Q1 2016 Malware Review



### How is a phishing email used to infect your computer with a ransomware?

A phishing email containing links to malicious websites - visiting such sites can drop a ransomware on your PC.

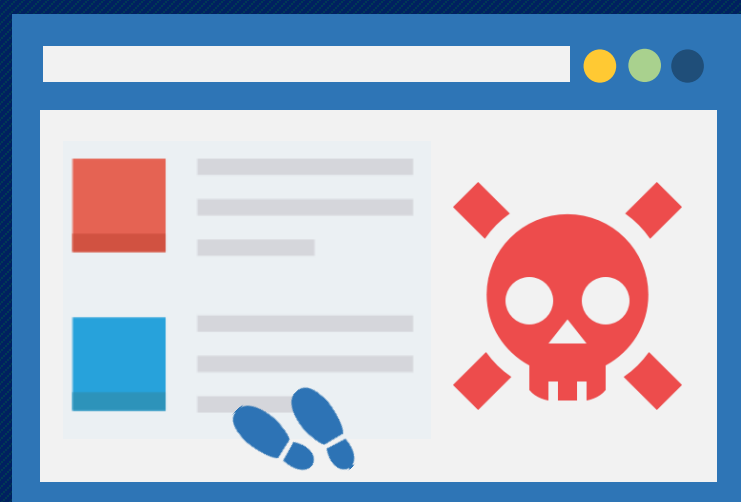
A phishing email carrying attachments hiding ransomware - Downloading such attachments will execute a ransomware on your PC. These attachments are usually MS Office docs such as Word, Excel, and PPTs, and PDFs.

To make a phishing email look more genuine and convincing, it is disguised as something that you'd expect – invoices, tax forms, letters from a co-employee or your boss, purchase receipts, etc.

# #2.

## COMPROMISED WEBSITES

An infected or a compromised website (in this case) is a webpage(s) where the attacker has hidden an exploit kit (a software designed to misuse software vulnerabilities).



When you visit such a site, this exploit kit will scan your web browser or other software for security vulnerabilities it is designed to exploit (security vulnerability is a weakness in your computer that an attacker can misuse). And if a vulnerability is found, the kit will drop the ransomware.

### How do you land up on a site compromised with an exploit kit?

By clicking on a link in a phishing email – the most common way

By clicking on a malicious advertisement

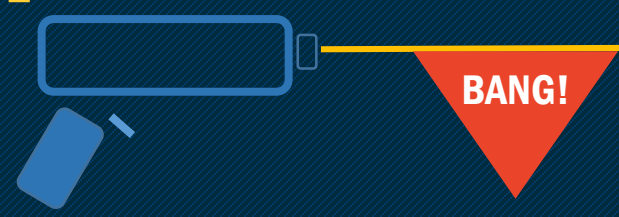


This attack is called **malvertisement** – ads loaded with malware.

Malicious ads do not only appear on shady websites, they target genuine websites too. This means, clicking on an ad on a legitimate website can also infect your computer with a ransomware.

**Case in point:** Malicious ads (containing the Angler exploit kit) appeared on The New York Times, the BBC, AOL, and the MSN homepage in 2016, delivering ransomware to the people visiting these websites.

## HOW DO YOU DEFEAT RANSOMWARE?



Staying safe from ransomware means preventing it from getting inside your computer. You can do this by...

**#1. NOT CLICKING** on links or downloading attachments from unknown or unexpected sources (even if the sender looks familiar).

**#2. PATCHING** all vulnerabilities in your Operating System and software by applying all recommended security updates.

**#3. PROTECTING** your computer with an antivirus that can block access to compromised websites and prevent ransomware from getting downloaded on the system.

**#4. BACKUP YOUR DATA** regularly. Consider storing them securely in multiple, offline locations. Should a ransomware infection occur, you can restore your data from these backups.

**#5. INSTALL AD-BLOCKERS** on your web browsers. This will reduce your risk on clicking on malicious or harmful advertisements.

STAY AWARE  
STAY SAFE



Sources  
blogs.quickheal.com | phishme.com |  
www.us-cert.gov | www.wired.com |  
www.securityaffairs.co