

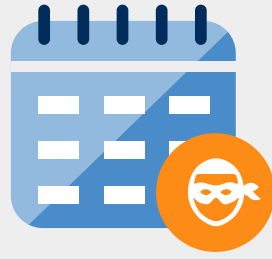
# RANSOMWARE: 3 SECONDS TO ENCRYPTION



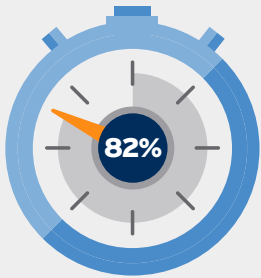
## SMBs AT RISK



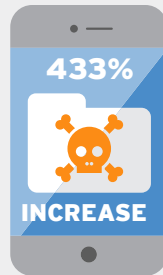
More than 70% of attacks **target small business**  
- National Cybersecurity Alliance



4 out of 5 **victims don't know** they have been hacked for weeks  
- Verizon Data Breach Investigations Report



Cyber attackers compromised 82% of victims **within minutes**  
- Verizon Data Breach Investigations Report



433% **increase in ransomware** incident reports over the past year  
- Arctic Wolf Research



RANSOMWARE IS ON PACE TO BE A **\$1 BILLION**  
A YEAR CRIME -FBI

SMBs BREACHED SPENT AN AVERAGE OF **\$879,582**  
DUE TO DAMAGE OR THEFT OF IT ASSETS  
-Ponemon Institute

## INFECTION TO ENCRYPTION IN 3 SECONDS



SECOND 0

User clicks on phishing email

SECOND 1.0

User unknowingly downloads ransomware

Ransomware unpacks and executes

SECOND 1.5

Ransomware downloads encryption keys

SECOND 2.0



ENCRYPTION COMPLETED

SECOND 2.5

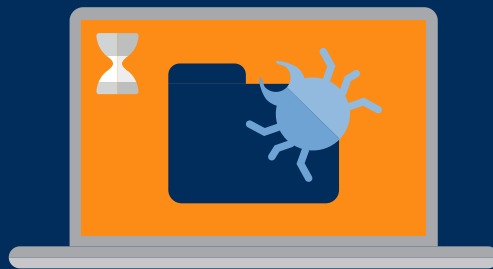
Scans computer to identify all attached drives

SECOND 3.0

File encryption begins



User gets ransom notification



## 5 WAYS TO PROTECT AGAINST RANSOMWARE



**NETWORK SEGMENTATION**  
Put critical data on separate network segments and consider internal firewalls or physical separation



**BACKUP AND RESTORE**  
Make sure you have a robust backup and process in place, test it to ensure you know how to use it and that the backup is working



**EMPLOYEE TRAINING**  
Train employees so they know what to look out for, security best practices, and how to identify threats



**STAY UP TO DATE**  
Being diligent in updating systems and software will help make the most of technology investments



**MONITOR, DETECT, RESPOND**  
Focus on threat detection, 24/7 monitoring and incident investigation and response to detect known and unknown attacks