

Cyberattack Survival: Prevention is the best protection

Yesterday's Attacks

Today's Attacks

What does
an attack
look like?



Hackers took a targeted approach and focused on enterprises because of their high-value data, such as financial records, that they could either sell or make openly accessible.

Hackers are still looking for data, but they now take an automated spray and pray approach because it's easier and much more lucrative.

How do they
get in?



They get in by hacking into databases and internal systems via root kits, key loggers and Trojans, bot net attacks, etc.

Today, hackers use advanced social engineering techniques to trick unsuspecting users into handing over confidential or sensitive data.

What data do
they steal?



Information that can be bought and sold (credit card numbers, bank accounts info, social security numbers, engineering plans and other intellectual property)

Information of value to your business that you will pay to get back (operational data, documents, research, budget information etc.)

Can your business afford a cyberattack?

3 in 5

SMBs have experienced a cyberattack in the last 12 months

20%

of those businesses attacked had to cease operations immediately

8 hours to 1 week

the time businesses took to wipe and restore infected computers

40%

of infections spread through the network to multiple endpoints

It can take hours, weeks, months or even years to restore systems and operations.

Ask yourself:

Can I afford to pay hundreds or even thousands of dollars from a cyberattack?

Can my business continue to operate if I don't have access to my business files?

What would three days of downtime cost?

How would a cyberattack impact my customers?

Would a cyberattack damage my business' reputation?

Prevention is the best protection!

Learn how to protect your business
with the **Good, Better, Best** prevention model

GOOD

BETTER

BEST

Back up files to an external drive or secure cloud



Back up to an external hard drive

Back up in two formats and keep a copy offsite

Use bare metal backup and/or file and folder backup stored in the cloud

Educate employees and create policies



Boost employee awareness

Implement mandatory cyberattack training/testing for employees

Train employees and create internal policies for reporting and handling cyberattacks

Update all software to the latest version



Keep your operating system (OS) up to date

Keep your OS and applications up to date

Keep your OS and applications up to date in addition to removing toolbars and freeware

Use multi-level antivirus protection



Use antivirus

Use antivirus with anti-spam

Use antivirus with anti-spam and link scanning.

Running your business should be your number one priority. Let us focus on your security.

Contact us today to find out how we can protect your business against cybercrime.

#securitysimplified