

CYBER SECURITY

12 Steps to Help Protect your Business
from Cyber Criminals.



What is Cybersecurity?

Cybersecurity for veterinary clinics is the practice of protecting a clinic's computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It is important for clinics to take cybersecurity seriously, as they are just as vulnerable to cyberattacks as larger businesses.



Why is it Important?

- Cybercrime is growing exponentially. The cost of cyber crime is expected to cost business \$8 trillion in 2023 and will grow to over \$10 trillion in 2025.
- In 2022
 - 76% of organizations were targeted by a ransomware attack
 - 64% were infected
 - 50% of these organizations were able to retrieve their data after paying the ransom.



Why is it Important for Small Businesses

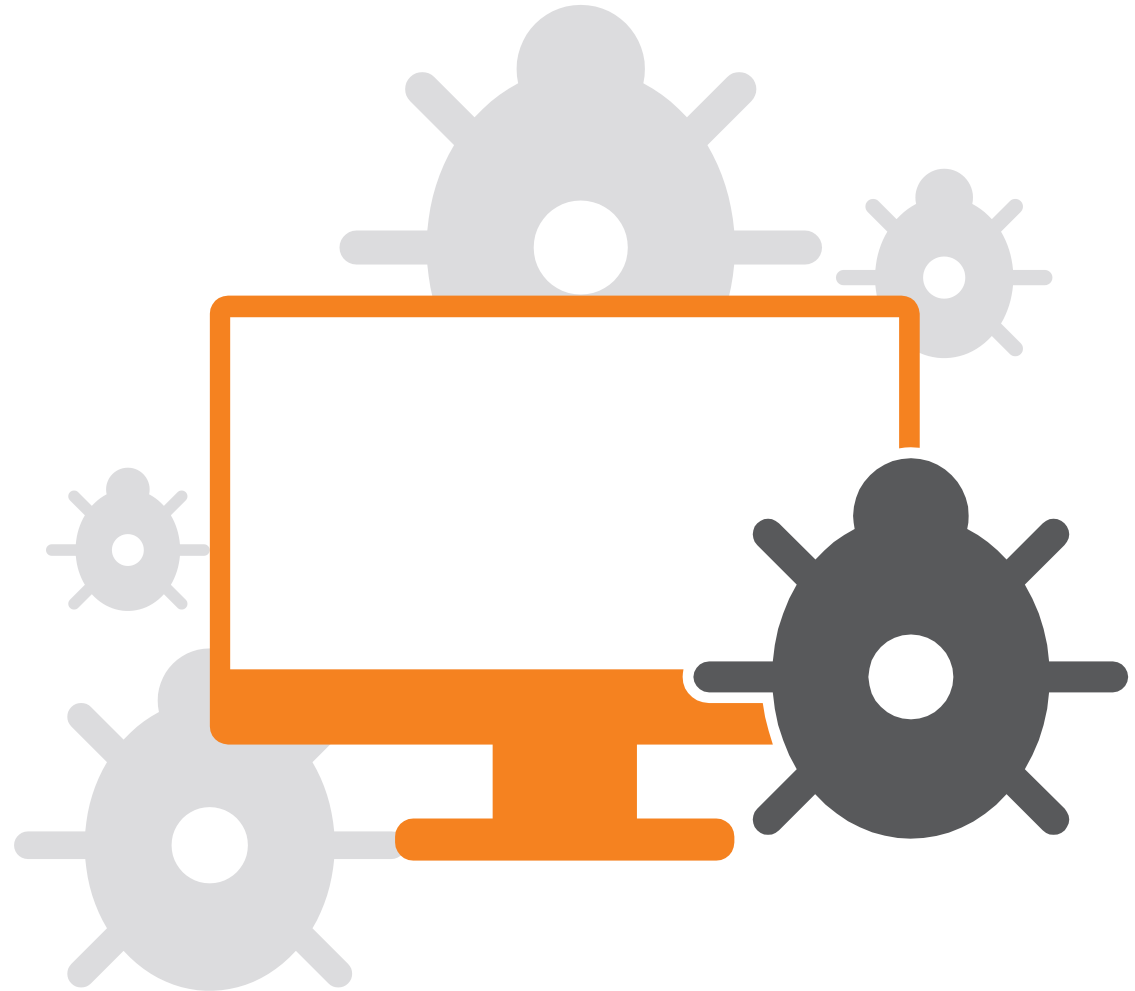
- 43% of cyber attacks target small businesses
- Small businesses spend an average of \$955,429 on restoring regular business after a successful attack
- 60% of small business that fall victim to a cyber attack go out of business within 6 months
- 54% of small business think they are too small for a cyber attack



Current Threats: Phishing

Phishing attacks occur when an attacker pretends to be a trusted contact, and entices a user to click a malicious link, download a malicious file, or give them access to sensitive information, account details or credentials.

Phishing is the preferred method used by hackers to gain access to your data and systems.



Current Threats: Malware

Malware is a term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.



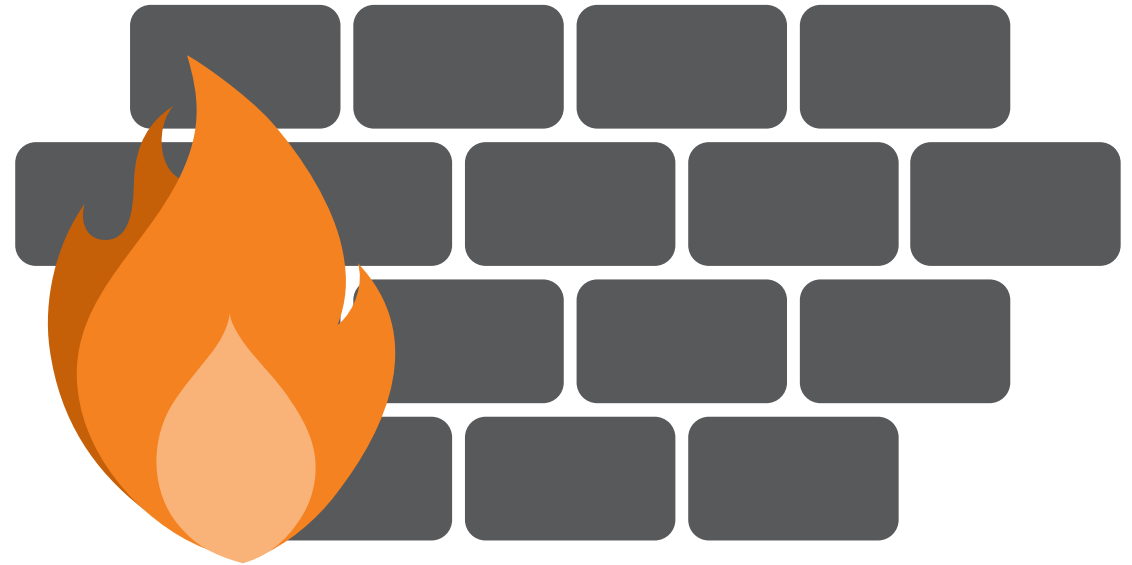
Current Threats: Ransomware

Ransomware involves encrypting company data so that it cannot be used or accessed, and then forcing the company to pay a ransom to unlock the data. This leaves businesses with a tough choice – to pay the ransom and potentially lose huge sums of money or cripple their services with a loss of data.



Current Threats: Weak Passwords

Many small businesses use multiple cloud based services, that require different accounts. These services often can contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts, can cause this data to become compromised.



Current Threats: Insider Threats

An insider threat is a risk to an organization that is caused by the actions of employees, former employees, business contractors or associates. These actors can access critical data about your company, and they can cause harmful effects through greed or malice, or simply through ignorance and carelessness.



Cyber Security is for Everybody

Big business, small business, mom and pop shop. If you're in business, you need to make cyber security a part of it.





Train
Employees





Install Anti Virus Software

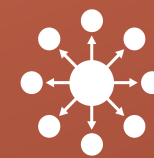




Create separate user accounts and limit access



Back up data
regularly



Use a password manager



Secure WiFi
network and
use a firewall



Strong
passwords



Multi-factor authentication

Control physical
access to computers



Keep software updated



Ensure 3rd parties are also secure





Consider cyber insurance



Ensure 3rd parties are also secure



Consider cyber insurance



Train Employees



Install Anti Virus Software



Keep software updated



Create separate user accounts and limit access



Control physical access to computers



Back up data regularly



Multi-factor authentication



Strong passwords



Secure WiFi network and use a firewall



Use a password manager



0010110000101001101001000001 001011000010100110
001010011010010000111000101 001010011010010000
010110000101001101001000011 010110000101001101
101001101001000011100010110 101001101001000011
001011000010100110100100001 001011000010100110
010100110100100001110001011 010100110100110100
001011000010100110100100001 001011000010100110
010000111000101100110010110 010000101101001101
010100110100100001110001011 010100110100110100
011011001011000010100110100 01101100101101001101
110010110000101001101001000 11001011000010100110
100001010011010010000111000 100001010011010011010011

Additional Information



Social Engineering Red Flags

Social Engineering Red Flags

FROM

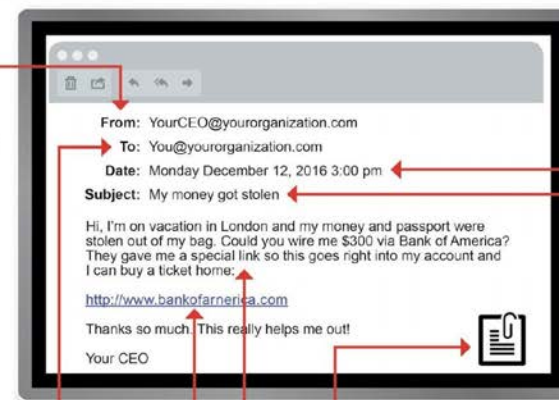
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they were **not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Additional Resources

Security Training

- Coursera: <https://www.coursera.org/search?query=cybersecurity%20for%20everyone>
- Phished: <https://phished.io/>
- KnowBe4: <https://www.knowbe4.com/>

Anti-Virus Software

- McAfee: <https://www.mcafee.com/en-us/abt/2023/pp/antivirus-ctl.html>
- BitDefender: <https://www.bitdefender.com/solutions/antivirus.html>

Backup Services

- Backblaze: <https://www.backblaze.com/cloud-backup>
- Crashplan: <https://www.crashplan.com/>
- IDrive: <https://www.idrive.com/>

Password Managers

- BitWarden: <https://bitwarden.com/>
- 1Password: <https://1password.com/>