In short, they are playing right into hackers’ hands. Multi-million-dollar attacks on famous companies get the headlines, but most cyberattacks target small businesses. For good reason: They invest less in cybersecurity, are less aware of threats and their losses don’t get the same attention.

“Small businesses have this idea that they’re too small to bother with,” says Mario Delapena, a Technology Advisor with Dell Small Business. “Attackers know they can get away with it. If they can get $1,500 from you in a ransomware attack, they’ll absolutely take it.”

43% of small businesses take no internet security precautions at all, and less than half train their employees in cybersecurity.


A change in perspective for small business

Instead of viewing cybersecurity as an expense, Delapena contends, small businesses should view it as an investment in their business’s health.

“In your personal health, you know you need to eat healthy and exercise,” he says. “You also need to know what to avoid. People take vitamins, buy exercise equipment, learn to cook healthy meals, cut back on junk food, avoid smoking and get enough sleep.

In cybersecurity terms, “healthy” living means:
- Respecting access security – setting strong passwords and making it a policy to change them regularly.
- Installing security software, firewalls, and securing access to hardware, using laptops featuring TPM 2.0 (Trusted Platform Module) technology, fingerprint readers and facial recognition.
- Practicing safe internet use, knowing not to download suspicious files or click links from strange emails.
- Investing in PCs powered by 8th gen Intel Core™ i5 vPro™ processors, which deliver hardware-enhanced security features.

What’s at risk in a cyberattack?

It’s important for small businesses to understand exactly what is at risk so they can accurately assess the value of cybersecurity.

There’s the direct financial risk if a hacker is able to extort, steal or scam money from a business or its employees. But for small businesses, the risk can go much deeper.

“I ask small businesses, what would you do if you couldn’t access your most important data?” says Delapena. “They have to think about the importance of efficiency and uptime. What if you had to shut down for a day? Or if all the files for a big project just went away?”

The effects tend to ripple outward. Employees might not get paid. Customers may have their own security compromised. And the harm to reputation can have a long-lasting effect.

With that perspective, the value-to-investment ratio for small businesses is often easier to understand.

Customers may have their own security compromised. And the harm to reputation can have a long-lasting effect. With that perspective, the value-to-investment ratio for small businesses is often easier to understand.

“The best thing you can do is be very cautious,” Delapena concludes. “These people are very inventive and creative and have the wherewithal to try new things.”

Top threats to small businesses – and how to defend against them

Phishing: Capturing usernames and passwords by directing victims to fake, but real-looking, login pages.

Defense: Train employees to be suspicious of unexpected emails and look at “from” addresses.

Data breaches: Hackers get into company files, where they can steal customer data, client work, intellectual property or financial data.

Defense: Strong passwords, computers with enhanced security features and gap-free network protection – lock down Wi-Fi and don’t let employees use private cloud storage to store work files.

Malware: Open a document, and voilà – a trojan is now sitting on your computer.

Defense: Install security software and regularly update the software.

Top threats to small businesses – and how to defend against them

Phishing: Capturing usernames and passwords by directing victims to fake, but real-looking, login pages.

Defense: Train employees to be suspicious of unexpected emails and look at “from” addresses.

Data breaches: Hackers get into company files, where they can steal customer data, client work, intellectual property or financial data.

Defense: Strong passwords, computers with enhanced security features and gap-free network protection – lock down Wi-Fi and don’t let employees use private cloud storage to store work files.

Malware: Open a document, and voilà – a trojan is now sitting on your computer.

Defense: Install security software and regularly update the software.

Small businesses have this idea that they’re too small to bother with.” says Mario Delapena, a Technology Advisor with Dell Small Business. “Attackers know they can get away with it. If they can get $1,500 from you in a ransomware attack, they’ll absolutely take it.”

43% of small businesses take no internet security precautions at all, and less than half train their employees in cybersecurity.