FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Cybersecurity for small business: Ransomware

Share This Page

Andrew Smith, Director, FTC Bureau of Consumer Protection
Nov 16, 2018

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Data Security | Small Business

Mention the word "ransomware" at a meeting of small business owners and you'll feel the temperature in the room drop by 20 degrees. A ransomware attack is a chilling prospect that could freeze you out of the files you need to run your business. When FTC staff met with business owners across the country, you cited ransomware as a particular concern. New resources from the FTC can help protect your company from this threat.

Ransomware: How it happens

What is a ransomware attack? It can start innocently enough. An employee clicks on a link, downloads an email attachment, or visits a website where malicious code is lurking in the background. With just one keystroke, they inadvertently install software that locks you out of your own files. The cyber crook then demands a ransom, often in the form of cryptocurrency. But even if you pay, there's no guarantee that hackers will live up to their end of the bargain. They may pocket the payment and vanish without unlocking your files. Meanwhile, the information you need to run your business – and confidential data about your customers and employees – is now in criminal hands.

How to protect your business

The best defense against ransomware is prevention. Keep your computer security in fighting form by installing the latest patches and updates. Consider additional means of protection like email authentication and intrusion prevention software, and set them to update automatically. (You may have to do that manually on mobile devices.)

Back up your data regularly by saving important files to a drive or server not connected to your network. And have a "What if . . . ." plan in place that outlines the steps you'll take if ransomware strikes.

Warn your staff about the potential consequences of casually clicking on a link or opening an unexpected attachment. Clue them in to how some cyber criminals use phishing emails that impersonate the look of business correspondence. Build into employee orientation and training some tips for protecting against ransomware, including this FTC factsheet, quiz, and video.

What to do if you're attacked

Implement that action plan. Limit the damage by immediately disconnecting the infected computers or devices from your network. Then report the attack right away to your local FBI office. If data or personal information was compromised, consider the advice in the FTC's Data Breach Response: A Guide for Business. Notify the affected parties. They could be at risk for identity theft.

Businesses who have been targets of ransomware often ask if they should pay the ransom. Law enforcement agencies don't recommend it, but it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. Of course, paying the ransom doesn't ensure that the hacker will restore your data. Deciding what's best for your business will be easier if you have those files securely backed up elsewhere.

Next week: Phishing