CYBERSECURITY FOR
SMALL BUSINESS

RANSOMWARE

Someone in your company gets an email.

It looks legitimate — but with one click on a link, or one download of an attachment, everyone is locked out of your network. That link downloaded software that holds your data hostage. That's a ransomware attack.

The attackers ask for money or cryptocurrency, but even if you pay, you don't know if the cybercriminals will keep your data or destroy your files. Meanwhile, the information you need to run your business and sensitive details about your customers, employees, and company are now in criminal hands. Ransomware can take a serious toll on your business.

HOW IT HAPPENS

Criminals can start a ransomware attack in a variety of ways.

Scam emails

with links and attachments that put your data and network at risk. These phishing emails make up most ransomware attacks.

Server vulnerabilities

which can be exploited by hackers.

Infected websites

that automatically download malicious software onto your computer.

Online ads

that contain malicious code — even on websites you know and trust.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR SMALL BUSINESS

HOW TO PROTECT YOUR BUSINESS

Have a plan

How would your business stay up and running after a ransomware attack? Put this plan in writing and share it with everyone who needs to know.

Back up your data

Regularly save important files to a drive or server that's not connected to your network. Make data backup part of your routine business operations.

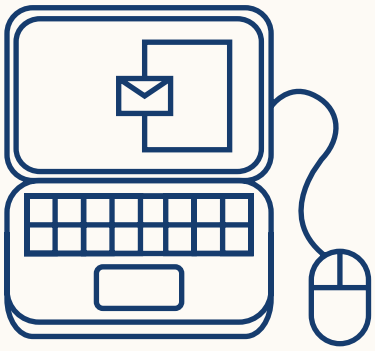
Keep your security up to date

Always install the latest patches and updates. Look for additional means of protection, like email authentication, and intrusion prevention software, and set them to update automatically on your computer. On mobile devices, you may have to do it manually.

Alert your staff

Teach them how to avoid phishing scams and show them some of the common ways computers and devices become infected. Include tips for spotting and protecting against ransomware in your regular orientation and training.

WHAT TO DO IF YOU'RE ATTACKED



Limit the damage

Immediately disconnect the infected computers or devices from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected.

Contact the authorities

Report the attack right away to your local FBI office.

Keep your business running

Now's the time to implement that plan. Having data backed up will help.

Should I pay the ransom?

Law enforcement doesn't recommend that, but it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. However, paying the ransom may not guarantee you get your data back.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties – they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business*. You can find it at FTC.gov/DataBreach.

LEARN MORE AT: FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

PHISHING

You get an email that looks like it's from someone you know.

It seems to be from one of your company's vendors and asks that you click on a link to update your business account. Should you click? Maybe it looks like it's from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.

HOW

PHISHING WORKS

You get an email or text

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

It looks real

It's easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

It's urgent

The message pressures you to act now — or something bad will happen.

What happens next

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

WHAT YOU CAN DO

Before you click on a link or share any of your sensitive business information:

Check it out

Look up the website or phone number for the company or person behind the text or email. Make sure that you're getting the real company and not about to download malware or talk to a scammer.

Talk to someone

Talking to a colleague might help you figure out if the request is real or a phishing attempt.

Make a call if you're not sure

Pick up the phone and call that vendor, colleague, or client who sent the email. Confirm that they really need information from you. Use a number you know to be correct, not the number in the email or text.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR

SMALL BUSINESS

HOW TO PROTECT YOUR BUSINESS

Back up your data

Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

Keep your security up to date

Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may have to do it manually.

Alert your staff

Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.

Deploy a safety net

Use email authentication technology to help prevent phishing emails from reaching your company's inboxes in the first place.

WHAT IF YOU FALL FOR A PHISHING SCHEME

Alert others

Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in a company.

Limit the damage

Immediately change any compromised passwords and disconnect from the network any computer or device that's infected with malware.

Follow your company's procedures

These may include notifying specific people in your organization or contractors that help you with IT.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business* (FTC.gov/DataBreach).

Report it

Forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme. And report it to the FTC at FTC.gov/Complaint.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security