



# Cybersecurity Education FTC Resources

Rosario Méndez  
Federal Trade Commission

# business.ftc.gov





**START WITH SECURITY**

A GUIDE FOR BUSINESS

LESSONS LEARNED FROM FTC CASES

FEDERAL TRADE COMMISSION

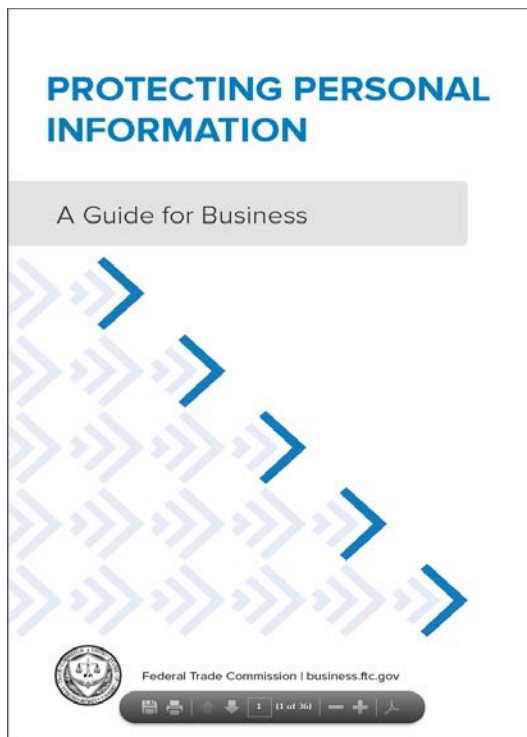
**SEGURIDAD**

UNA GUÍA PARA NEGOCIOS

LECCIONES DE LOS CASOS DE LA FTC.

LA COMISIÓN FEDERAL DE COMERCIO

# PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS



1. Take Stock.
2. Scale Down
3. Lock It.
4. Pitch It.
5. Plan Ahead.

# DATA BREACH RESPONSE: A GUIDE FOR BUSINESS



Guidance for businesses – and government – if you discover a data breach

Explains steps to take & who to notify



**CYBERSECURITY**

for small business

# NEW CYBERSECURITY FOR SMALL BUSINESS EDUCATION CAMPAIGN

12 modules

- Fact Sheet
- Quiz
- Video

Discussion Guide How to train your employees?

# 12 MODULES

Cybersecurity Basics

NIST Cybersecurity  
Framework

Physical Security

Ransomware

Phishing

Business Email Imposters

Tech Support Scams

Vendor Security

Cyber Insurance

Email Authentication

Hiring a Web Host

Secure Remote Access



CYBERSECURITY FOR  
SMALL BUSINESS

# SECURE REMOTE ACCESS

## Employees and vendors may need to connect to your network remotely.

Put your network's security first. Make employees and vendors follow strong security standards before they connect to your network. Give them the tools to make security part of their work routine.

### HOW TO PROTECT DEVICES

Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips — and make sure your employees and vendors do as well:

Always change any pre-set router passwords and the default name of your router. And keep the router's software up-to-date; you may have to visit the router's website often to do so.

Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. Check your operating system for this option, which will protect any data stored on the device if it's lost or stolen. This is especially important if the device stores any sensitive personal information.

Change smartphone settings to stop automatic connections to public Wi-Fi.

Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.



CYBERSECURITY FOR  
SMALL BUSINESS

### HOW TO CONNECT REMOTELY — TO THE NETWORK

Require employees and vendors to use secure connections when connecting remotely to your network. They should:



Use a router with WPA2 or WPA3 encryption when connecting from their homes. Encryption protects information sent over a network so that outsiders can't read it. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.

Only use public Wi-Fi when also using a virtual private network (VPN) to encrypt traffic between their computers and the internet. Public Wi-Fi does not provide a secure internet connection on its own. Your employees can get a personal VPN account from a VPN service provider, or you may want to hire a vendor to create an enterprise VPN for all employees to use.

### WHAT TO DO TO MAINTAIN SECURITY —

#### Train your staff:

Include information on secure remote access in regular trainings and new staff orientations.



Have policies covering basic cybersecurity, give copies to your employees, and explain the importance of following them.

Before letting any device — whether at an employee's home or on a vendor's network — connect to your network, make sure it meets your network's security requirements.

Tell your staff about the risks of public Wi-Fi.

#### Give your staff tools that will help maintain security:

- Require employees to use unique, complex network passwords and avoid unattended, open workstations.
- Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.
- Consider creating a VPN for employees to use when connecting remotely to the business network.
- If you offer Wi-Fi on your business premises for guests and customers, make sure it's separate from and not connected to your business network.
- Include provisions for security in your vendor contracts, especially if the vendor will be connecting remotely to your network.

LEARN MORE AT:  
[FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)



LEARN MORE AT:  
[FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)



---

**2. What is a common way to help protect devices connected to the company network?**

**A.** Only use laptops and other mobile devices with full-disk encryption.

**B.** Change your smartphone settings to let your devices connect automatically to public Wi-Fi.

**C.** Let guests and customers use the same secure Wi-Fi that you use.

**D.** Use the router's pre-set password so you won't forget it.

---

## 2. What is a common way to help protect devices connected to the company network?

**A.** Only use laptops and other mobile devices with full-disk encryption.

**B.** Change your smartphone settings to let your devices connect automatically to public Wi-Fi.

**C.** Let guests and customers use the same secure Wi-Fi that you use.

**D.** Use the router's pre-set password so you won't forget it.

**This is correct!** Full-disk encryption will protect any data stored on the device if your device is lost or stolen.

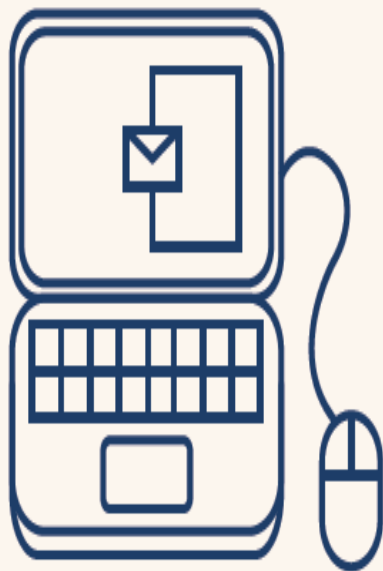
**CYBERSECURITY FOR**

**SMALL BUSINESS**

**RANSOMWARE**



# 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.

## 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](https://www.ftc.gov/DataBreach).

## 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.

# 12 MODULES

Cybersecurity Basics

NIST Cybersecurity  
Framework

Physical Security

Ransomware

Phishing

Business Email Imposters

Tech Support Scams

Vendor Security

Cyber Insurance

Email Authentication

Hiring a Web Host

Secure Remote Access

# TALKING CYBERSECURITY

## WITH YOUR EMPLOYEES



### **Learn about cybersecurity**

Read the cybersecurity fact sheets at [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness). Consider how the information applies to your business.

---



### **Talk about cybersecurity**

Talk about cybersecurity with your employees, vendors, and others involved in your business. Share with them the information at [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness).

---



### **Use online videos and quizzes**

Ask your employees to watch the videos at [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness). Use online quizzes to test their understanding of the cybersecurity topics.



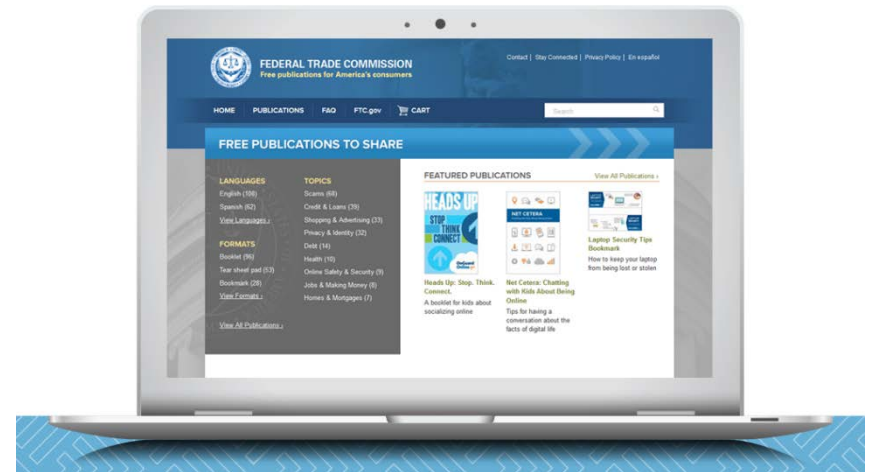
**CIBERSEGURIDAD PARA**


**PEQUEÑOS NEGOCIOS**

**CÓMO HABLAR  
DE CIBERSEGURIDAD**

**CON SUS EMPLEADOS**

# bulkorder.ftc.gov





**I speak for myself,  
and not for the FTC.**

# QUESTIONS?

## **Rosario Méndez**

Federal Trade Commission

[rmendez@ftc.gov](mailto:rmendez@ftc.gov)

## **FTC.gov/SmallBusiness**

- Small business info
- Scams
- Cybersecurity

## **Business.FTC.gov**

- all business info
- Sign up for blog

## **FTC.gov/Bulkorder**

- Order free publications

