SERIES OVERVIEW

- Raise awareness about cybersecurity’s importance
- Help keep data from bad actors
- Understand reality of socially engineering
- Understand and learn steps to mitigate risks
- Reduce volume and impact of attacks
- No program leads to 100% success

SERIES OVERVIEW: AWARENESS & TRAINING LEVELS

- Ensure all users are made aware of security risks, applicable policies, standards and procedures
- Ensure personnel are trained to carry out their assigned security-related duties and responsibilities
- Provide security awareness training on recognizing and reporting potential indicators of insider threat
- Provide awareness training focused on recognizing and responding to threats from social engineering, etc. (update at least annually or when there are significant changes)
- Include practical exercises aligned with current threat scenarios

7

8

9
IN THIS PRESENTATION

- Company Overview
- Series Overview
- Information Security Recap
- Social Engineering
- Phishing
- COVID-19 Phishing Statistics

INFORMATION SECURITY RECAP

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Maersk shipping systems experienced a significant interruption after getting hit with the Notpetya ransomware. Their resuming of normal business operations was aided with this part of the information security model.

- a) Disaster Recovery
- b) Physical Security
- c) Crossing Fingers
- d) Taking a Vacation
Before hiring Josh, a background check revealed he spent time in prison for credit card fraud. This check is what part of the information security model?

Lumina ensures that her clients and employees’ personal information is protected. She focuses on what part of information security?
Lumina ensures that her clients and employees’ personal information is protected. She focuses on what part of information security?

a) Privacy  b) Cybersecurity  c) Personnel  d) Physical

At the end of work, Brock forgot to lock his sensitive documents in his file cabinets or secure his computer to his desk. When he returned the next day, his computer and documents were missing. Brock demonstrated poor…

a) Disaster Recovery  b) Physical Security  c) Privacy  d) Personnel Security
Mia wrote her company’s _______security plan, which set clear guidelines on what was allowed and clearly defined the responsibilities, authorizations, and disciplinary actions in case of breaches.

a) Privacy  b) Cybersecurity  c) Personnel  d) Operational
The use of human interaction, social skills and manipulation by an attacker to obtain or compromise information about an organization or its computer systems.

“Upwards of 90-plus percent of breaches on networks are from some sort of social engineering effort.”

- Rosa Smothers, KnowBe4

Attacker may seem unassuming or respectable
Attacker asks questions to piece together information
May gather information from multiple sources in organization
Manipulates human natural tendency to trust
“Human nature is to be lazy….I mean efficient!”

• Person to Person Contact
• Attempt to Influence an Action
• Attempt to Retrieve Information
• Using Computer Software-Based Interaction
• Attempt to Influence an Action
• Attempt to Retrieve Information
• Attempt to Install Malware
SOCIAL ENGINEERING

- Attackers
- Plan & Research
- Personal Info
- Associates
- Clients
- Family
- Business Info

Compliance is influenced, not forced.

Emotions motivate behavior.

People make decisions based on maximizing pleasure and minimizing pain.

Employers should align awareness and compliance with employees' emotional goals.

“Hackers find more success with organizations where employees are under appreciated, overworked and underpaid. Why would anyone in an organization like that care enough to think twice before clicking on a phishing email.”

- James Scott
SOCIAL ENGINEERING

- Validate people are who they say they are
- Authorize before clicking on links or returning calls
- Only provide information to authorized individuals
- Do not give out your password

IN THIS PRESENTATION

- Company Overview
- Series Overview
- Information Security Recap
- Social Engineering
- Phishing
- COVID-19 Phishing Statistics

PHISHING

- No Phishing allowed
A form of social engineering using email or malicious websites to solicit personal information by posing as a trustworthy organization.

"94% of malware is delivered by email."

• Leverages voice communication
• Entice victim to call a number and divulge sensitive information
• Can use Voice over Internet Protocol (VoIP) to spoof caller identity
• 83% of information security professionals reported vishing attempts in 2019
Smishing

- Exploits SMS or text messages
- Texts contain links to malicious websites, email addresses or phone numbers
- 84% of information security professionals reported smishing attempts in 2019

Mass-Scale Phishing

- Fraudsters cast a wide net of attacks that are not highly targeted

Spear Phishing

- Fraudsters tailor attacks to a specific victim or group of victims using personal details

Whaling

- Fraudsters target a "big" victim within a company, for example, CEO, CFO or other executive

90% of organizations faced targeted phishing attacks in 2019

- Proofpoint
Attacker take advantage of current events like:
- Natural Disasters (Hurricane Katrina/Wildfires)
- Economic Concerns (IRS Scams)
- Major Political Elections
- Holidays
- Epidemics and Health Scares (H1N1/COVID-19)

Common Indicators of Phishing Attempts
- Suspicious Sender's Address
- Generic Greetings and Signature
- Spoofed Hyperlinks and Websites
- Spelling and Layout
- Suspicious Attachments
CAUTION: This e-mail originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Dear citizen,

Orders of our President Tedros Adhanom and his august office.
PHISHING

10/19/20

PHISHING

- NCOVID outbreak has reached epidemic proportions
- Conventional health care strategies have failed in containing the disease
- The future of healthcare systems looks bleak as the strain on these systems is becoming unbearable
- The office of our president is monitoring the situation and will issue periodic updates on the situation.

PHISHING

I am hereby requesting you to download the attached...

PHISHING

You will also get a free WHO NCOVID healthcare kit if you sign and share this document over the next 15 hours.
Avoid Being a Victim
- Be suspicious of unsolicited calls, visits or emails
- Be certain before providing personal information
- Don’t reveal personal or financial info in email
- Don’t respond to emails or click links requesting this info
- Check website’s security before sending sensitive information

Independently verify email legitimacy
- Install and maintain anti-virus software, firewalls and email filters
- Use anti-phishing features in email client and web browser
- Enforce multi-factor authentication

If You Think You are a Victim...
- Immediately report to appropriate people in your organization
- Contact financial institution and close any compromised accounts
- Immediately change any exposed or reused passwords
- Look for signs of identity theft
- Consider reporting to the police and Federal Trade Commission
PHISHING

If You Think You are a Victim...

Forward phishing emails to the Anti-Phishing Working Group
reportphishing@apwg.org

And to the Federal Trade Commission at
FTC.gov/Complaint.

PHISHING RECAP

Which one of these statements is correct?

a) If you get an email that looks like it’s from someone you know, you can click on any
   links as long as you have a spam blocker and anti-virus protection
b) You can trust an email really comes from a client if it uses the client’s logo and
   contains at least one fact about the client that you know to be true.
c) If you get a message from a colleague who needs your network password, you
   should never give it out unless the colleague says it’s an emergency.
d) If you get an email from Human Resources asking you to provide personal
   information right away, you should check it out first to make sure they are who they
   say they are.

PHISHING RECAP

Which one of these statements is correct?

a) If you get an email that looks like it’s from someone you know, you can click on any
   links as long as you have a spam blocker and anti-virus protection
b) You can trust an email really comes from a client if it uses the client’s logo and
   contains at least one fact about the client that you know to be true.
c) If you get a message from a colleague who needs your network password, you
   should never give it out unless the colleague says it’s an emergency.
d) If you get an email from Human Resources asking you to provide personal
   information right away, you should check it out first to make sure they are who they
   say they are.
An email from your boss asks for the name, addresses, and credit card information of the company’s top clients. The email says it’s urgent and to please reply right away. You should reply right away. True or False?

True  False

An email from your boss asks for the name, addresses, and credit card information of the company’s top clients. The email says it’s urgent and to please reply right away. You should reply right away. True or False?

True  False

You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should:

a) Reply to the text to confirm that you really need to renew your password.
b) Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.
c) Click on the link. If it takes you to the vendor’s website, then you’ll know it’s not a scam.
d) All of the above

a  b  c  d
PHISHING RECAP

You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should:

a) Reply to the text to confirm that you really need to renew your password.
b) Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.
c) Click on the link. If it takes you to the vendor’s website, then you’ll know it’s not a scam.
d) All of the above

a b c d

PHISHING RECAP

Email authentication can help protect against phishing attacks. True or False?

True False
**PHISHING RECAP**

If you fall for a phishing scam, what should you do to limit the damage?

- a) Delete the phishing email.
- b) Unplug the computer. This will get rid of any malware.
- c) Change any compromised passwords.
- d) None of the above

**PHISHING RECAP**

If you fall for a phishing scam, what should you do to limit the damage?

- a) Delete the phishing email.
- b) Unplug the computer. This will get rid of any malware.
- c) Change any compromised passwords.
- d) None of the above

**IN THIS PRESENTATION**

- Company Overview
- Series Overview
- Information Security Recap
- Social Engineering
- Phishing
- COVID-19 Phishing Statistics
**COVID-19 Phishing Statistics**

- 667% Increase in COVID-19 Phishing Attacks
- Scammers Preying on Coronavirus Fears
- Fake Links, Emails, Texts, Social Media Posts
- Phony Promotions of Awareness & Prevention
- Requests to Donate to Victims
- Bogus Product Offerings and Treatment Advice

---

**Top National COVID-19 Crime Reports as of October 14, 2020**

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>123,317</td>
</tr>
<tr>
<td>Other</td>
<td>42,581</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>32,522</td>
</tr>
<tr>
<td>Do Not Call</td>
<td>7,707</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
</tbody>
</table>

**As of October 14, 2020, the U.S. had $160,750,000 of total COVID-19-related losses due to fraud**
As of October 14, 2020, New Mexico had $470,000 of total COVID-19–related losses due to fraud.
COVID-19 PHISHING STATISTICS
Top Reports for New Mexico, as of October 14, 2020

5 Things to Avoid COVID-19 Scams
- Ignore offers for vaccinations and home test kits
- Hang up on robocalls
- Watch out for phishing emails and text messages
- Research before you donate
- Stay in the know

SUMMARY

QUIZ
SUMMARY QUIZ

The percentage of organizations that faced targeted phishing attacks in 2019

a) 30%  b) 50%  c) 70%  d) 90%

This text message is an example of what type of social engineering?

a) Vishing  b) Smishing  c) Phishing  d) Wishing
SUMMARY QUIZ

This text message is an example of what type of social engineering?

a) Vishing  b) Smishing  c) Phishing  d) Wishing

82

SUMMARY QUIZ

This type of social engineering uses Voice over Internet Protocol (VoIP) to spoof caller identity.

a) Vishing  b) Smishing  c) Phishing  d) Wishing

83

SUMMARY QUIZ

This type of social engineering uses Voice over Internet Protocol (VoIP) to spoof caller identity.

a) Vishing  b) Smishing  c) Phishing  d) Wishing

84
Social Engineering is well planned. Attackers may research which of the following?

a) Business Info  b) Client Info  c) Personal Info  d) All of the Above

A proactive training & awareness program should be updated when there are significant changes to the threat or at least

a) Daily  b) Weekly  c) Monthly  d) Annually
A proactive training & awareness program should be updated when there are significant changes to the threat or at least ________.

a) Daily  b) Weekly  c) Monthly  d) Annually

SUMMARY

Be wary of unsolicited attachments, even from people you know

Trust your instincts

Save and scan any attachments before opening them

SUMMARY

Disable option to automatically download attachments

Create separate accounts on your computer

Keep software up to date
SUMMARY
THINK BEFORE YOU CLICK

SUMMARY: CYBER SECURITY MONTH
DO YOUR PART.
#BECYBERSMART

SUMMARY: NEXT SESSION
SESSION 4: CONTROLS & PROTECTIONS
THURSDAY, OCTOBER 22, 2020
11:30 AM
THANK YOU!

TILLMAN CYBER SERVICES, LLC

AMERICA'S SBDC
NEW MEXICO

94
CYBERSECURITY FOR SMALL BUSINESS

CYBERSECURITY BASICS

Cyber criminals target companies of all sizes. Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT YOUR FILES & DEVICES

Update your software
This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files
Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords
Use passwords for all laptops, tablets, and smartphones. Don’t leave these devices unattended in public places.

Encrypt devices
Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication
Require multi-factor authentication to access areas of your network with 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.
PROTECT YOUR WIRELESS NETWORK

Secure your router
Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption
Make sure your router offers WPA2 or WPA3 encryption, and that it’s turned on. Encryption protects information sent over your network so it can’t be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords
A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don’t share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff
Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don’t attend, consider blocking their access to the network.

Have a plan
Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC’s Data Breach Response: A Guide for Business gives steps you can take. You can find it at FTC.gov/DataBreach.

LEARN MORE AT: FTC.gov/SmallBusiness
A scammer sets up an email address that looks like it’s from your company. Then the scammer sends out messages using that email address. This practice is called spoofing, and the scammer is what we call a business email imposter.

Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, your company has a lot to lose. Customers and partners might lose trust and take their business elsewhere — and your business could then lose money.

**HOW TO PROTECT YOUR BUSINESS**

**Use email authentication**
When you set up your business’s email, make sure the email provider offers email authentication technology. That way, when you send an email from your company’s server, the receiving servers can confirm that the email is really from you. If it’s not, the receiving servers may block the email and foil a business email imposter.

**Keep your security up to date**
Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

**Train your staff**
Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.
WHAT TO DO
IF SOMEONE SPOOFS YOUR COMPANY’S EMAIL

Report it
Report the scam to local law enforcement, the FBI’s Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also 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).

Notify your customers
If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks. You don’t want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. If your customers’ data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff
Use this experience to update your security practices and train your staff about cyber threats.

LEARN MORE AT:
FTC.gov/SmallBusiness
Email authentication technology makes it a lot harder for a scammer to send phishing emails that look like they’re from your company.

Using email authentication technology makes it a lot harder for scammers to send phishing emails. This technology allows a receiving server to verify an email from your company and block emails from an imposter — or send them to a quarantine folder and then notify you about them.

**WHAT TO KNOW**

Some web host providers let you set up your company’s business email using your domain name (which you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. Without email authentication, scammers can use that domain name to send emails that look like they’re from your business. If your business email uses your company’s domain name, make sure that your email provider has these three email authentication tools:

**Sender Policy Framework (SPF)**

Sends other servers which servers are allowed to send emails using your business’s domain name. So when you send an email from name@yourbusiness.com, the receiving server can confirm that the sending server is on an approved list. If it is, the receiving server lets the email through. If it can’t find a match, the email can be flagged as suspicious.

**Domain Keys Identified Mail (DKIM)**

Puts a digital signature on outgoing mail so servers can verify that an email from your domain actually was sent from your organization’s servers and hasn’t been tampered with in transit.

**Domain-based Message Authentication, Reporting & Conformance (DMARC)**

Is the essential third tool for email authentication. SPF and DKIM verify the address the server uses “behind the scenes.” DMARC verifies that this address matches the “from” address you see. It also lets you tell other servers what to do when they get an email that looks like it came from your domain, but the receiving server has reason to be suspicious (based on SPF or DKIM). You can have other servers reject the email, flag it as spam, or take no action. You also can set up DMARC so that you’re notified when this happens.

It takes some expertise to configure these tools so that they work as intended and don’t block legitimate email. Make sure that your email hosting provider can set them up if you don’t have the technical knowledge. If they can’t, or don’t include that in their service agreement, consider getting another provider.

**LEARN MORE AT:**

FTC.gov/SmallBusiness
WHAT TO DO IF YOUR EMAIL IS SPOOFED

Email authentication helps keep your business’s email from being used in phishing schemes because it notifies you if someone spoofs your company’s email. If you get that notification, take these actions:

### Report it

Report the scam to local law enforcement, the FBI’s Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can 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).

### Notify your customers

If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks: you don’t want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. And if your customers’ data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

### Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

LEARN MORE AT: FTC.gov/SmallBusiness
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**

**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.
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
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.

- **Infected websites** that automatically download malicious software onto your computer.

- **Server vulnerabilities** which can be exploited by hackers.

- **Online ads** that contain malicious code — even on websites you know and trust.
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.

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.

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.

LEARN MORE AT:
FTC.gov/SmallBusiness
TECH SUPPORT SCAMS

You get a phone call, pop-up, or email telling you there’s a problem with your computer. Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

HOW THE SCAM WORKS

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn’t one.

The scammers may then:

- Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it
- Install malware that gives them access to your computer and sensitive data, like user names and passwords
- Try to sell you software or repair services that are worthless or available elsewhere for free
- Try to enroll you in a worthless computer maintenance or warranty program
- Ask you to pay with a credit card or gift card for phony services or services available elsewhere for free
- Direct you to websites and ask you to enter credit card, bank account, and other personal information
HOW TO PROTECT YOUR BUSINESS

If a caller says your computer has a problem, hang up. A tech support call you don’t expect is a scam — even if the number is local or looks legitimate. These scammers use fake caller ID information to look like local businesses or trusted companies.

If you get a pop-up message to call tech support, ignore it. Some pop-up messages about computer issues are legitimate, but do not call a number or click on a link that appears in a pop-up message warning you of a computer problem.

If you’re worried about a virus or other threat, call your security software company directly, using the phone number on its website, the sales receipt, or the product packaging. Or consult a trusted security professional.

Never give someone your password, and don’t give remote access to your computer to someone who contacts you unexpectedly.

WHAT TO DO IF YOU’RE SCAMMED

If you shared your password with a scammer, change it on every account that uses this password. Remember to use unique passwords for each account and service. Consider using a password manager.

Get rid of malware. Update or download legitimate security software. Scan your computer, and delete anything the software says is a problem. If you need help, consult a trusted security professional.

If the affected computer is connected to your network, you or a security professional should check the entire network for intrusions.

If you bought bogus services, ask your credit card company to reverse the charges, and check your statement for any charges you didn’t approve. Keep checking your credit card statements to make sure the scammer doesn’t try to re-charge you every month.

Report the attack right away to the FTC at FTC.gov/Complaint.

LEARN MORE AT:
FTC.gov/SmallBusiness
Here are 5 things you can do to avoid a Coronavirus scam:

1. **Ignore offers for vaccinations and home test kits.**
   Scammers are selling products to treat or prevent COVID-19 without proof that they work.

2. **Hang up on robocalls.**
   Scammers use illegal sales call to get your money and your personal information.

3. **Watch out for phishing emails and text messages.**
   Don’t click on links in emails or texts you didn’t expect.

4. **Research before you donate.**
   Don’t let anyone rush you into making a donation. Get tips on donating wisely at ftc.gov/charity.

5. **Stay in the know.**
   Go to ftc.gov/coronavirus/scams for the latest information on scams. Sign up to get FTC’s alerts at ftc.gov/subscribe.

If you see a scam, report it to ftc.gov/complaint
A contact tracer from your state health department might call if you’ve been exposed to COVID-19. But scammers are pretending to be contact tracers, too. Here’s how you can spot the scam.

**Real contact tracers won’t ask you for money.**
- Only scammers insist on payment by gift card, money transfer, or cryptocurrency.

**Contact tracing doesn’t require your bank account or credit card number.**
- Never share account information with anybody who contacts you asking for it.

**Legitimate contact tracers will never ask for your Social Security number.**
- Never give any part of your Social Security number to anyone who contacts you.

**Your immigration status doesn’t matter for contact tracing, so real tracers won’t ask.**
- If they do, you can bet it’s a scam.

**Do not click on a link in a text or email.**
- Doing so can download malware onto your device.

Talking to a real contact tracer helps stop the spread of COVID-19. Reporting scammers helps stop them, too. Report fake contact tracers to your state and at [ftc.gov/complaint](http://ftc.gov/complaint).

For more information about contact tracing visit your state health department’s website and [ftc.gov/coronavirus/scams](http://ftc.gov/coronavirus/scams).