Scam Prevention Guide

Protecting yourself in an online world

Lemon Bay Computer Service

30 N Elm St

Englewood, FL 34223

(941) 548-1322

info@lemonbaycomputerservice.com

www.lemonbaycomputerservice.com

Recognize scams.
Protect your accounts and devices.
Keep control over your privacy.

A practical guide for consumers and older adults

Prepared by Lemon Bay Computer Service

Scammers target people of every age and skill level. Their messages can look professional, and their stories can sound convincing. Being targeted is not your fault. Asking for help early is a smart step.

STOP. CHECK. ASK.

• **Stop:** Do not click, pay, share a code, or allow remote access while someone is pressuring you.

• **Check:** Contact the organization using its official app, a saved trusted website, or a number on your card or statement.

• **Ask:** Talk to a trusted person before acting. A demand to keep the situation secret is a warning sign.

Already gave someone access?

Turn to page 8. Disconnect the affected device from the internet, contact your bank promptly from a trusted device or phone, and arrange a professional inspection.

Your local help

Lemon Bay Computer Service
30 N Elm St, Englewood, FL 34223
(941) 548-1322
Monday-Friday, 9am-5pm

Inside: Email and texts 3 | Facebook 4 | Phone calls 5 | Fake support and remote access 6 | Passwords and two-factor authentication 7 | Recovery 8 | Safety checklist 9 | References 10

1. Email and text messages

Phishing is a message designed to trick you into giving away information, sending money, or opening something harmful.

Recognize the pressure

• An unexpected bill, delivery fee, unpaid toll, refund, prize, or account warning asks you to act immediately.

• A familiar name or logo does not prove who sent the message. Correct spelling and personal details do not prove it is real either.

Before following a link

• Open the company's app yourself or type its known website address. Check your account there instead of using the message's link.

• On a computer, hovering over a link can reveal a different destination. This is only a clue, not proof of safety. On a phone, avoid opening an uncertain link just to investigate it.

• A padlock or https means the connection is encrypted; it does not mean the business is honest. Short links and QR codes can hide the destination.

• Do not open unexpected attachments or enable macros or other active content at a stranger's request. Confirm unexpected documents with the sender another way.

Example: “Your package cannot be delivered. Pay $1.95 here.”
Safer response: Open the carrier's official app or website and check your tracking number.

Handle suspicious texts

Do not reply, including with “STOP,” to a suspected scam. Use your phone's Report Junk option, block the sender, and delete the message. In the U.S., you can forward scam texts to 7726 (SPAM).

Sources: FTC phishing and spam-text guidance; Microsoft phishing guidance [1-3]. See the reference list on page 10.

2. Facebook and Messenger links

A message from a friend can come from a stolen account. An advertisement, familiar photograph, or large number of followers is not a guarantee of safety.

Be cautious with these messages

• “Is this you in this video?” or “Look who died” followed by a link.

• “Your Facebook page will be deleted” with a link to appeal or verify your password.

• An unusually cheap item, giveaway, investment, or urgent request for money from a friend.

Check without using the link

• Call the friend using a number you already know. Do not verify by replying to the same possibly stolen account.

• Open Facebook directly. Check account notices through its own settings or Help Center rather than a message's login page.

• Do not enter your Facebook password on a site reached through an unexpected message. Never send someone a login code or scan an unfamiliar account-linking QR code.

• For shopping, examine the seller and offer carefully. Avoid pressure to pay outside the platform or by gift card, wire transfer, or cryptocurrency.

Example: A friend says, “I need your six-digit code to recover my account.”
Safer response: Do not share it. The code may give them access to *your* account.

If you clicked

Close the page. If you entered a password or code, use a trusted device to change the password, review signed-in devices, and remove unfamiliar sessions. Report the message or account in Facebook. Warn friends if your account sent scam messages.

Sources: Meta account security, scam prevention, and account-linking guidance [4-6]. See the reference list on page 10.

3. Phone calls and convincing stories

Caller ID can be faked. A call can display your bank's name, a local number, or a government agency even when a scammer is calling.

End the call when someone demands...

• Immediate payment, secrecy, or that you stay on the phone while visiting your bank.

• Gift cards, cryptocurrency, cash handed to a courier, or a transfer to a supposedly “safe” account.

• Your password, a login verification code, or remote control of your computer or phone.

• Payment to prevent arrest, collect a prize, or fix an unexpected computer emergency.

Use a trusted callback

Hang up. Call the number printed on your bank card or statement, or a number you independently know is correct. Do not use a callback number provided by the caller. You do not need to be polite to someone pressuring you.

A sentence to practice:
“I do not handle unexpected requests on the phone. I will contact the organization myself.”

When the story involves family

A caller may claim a relative is hurt or in trouble. Pause and call that relative or another trusted family member using a saved number. A familiar-sounding voice is not enough to verify the story. Agree on a family verification phrase in advance, and keep it private.

Let support help you slow down

Let unknown callers go to voicemail. Keep trusted numbers on paper near your phone. Ask a family member or trusted helper to review confusing requests with you. Never let embarrassment delay reporting a loss.

Sources: FTC phone scams and avoiding scams [7-8]. See the reference list on page 10.

4. Fake tech support and remote access

The first search result is not necessarily official support. Scammers buy ads and manipulate search listings. When you search “Microsoft support” or “HP printer support,” a fake support website or phone number can appear at or near the top, including in sponsored results.

Go directly to **support.microsoft.com** or **support.hp.com** by typing the address yourself. Use support options there or contact a technician you already trust. Do not rely on a number in an ad, pop-up, or unexpected message.

A frightening website is not a diagnosis

A page may sound an alarm or claim your device is infected. Do not call its number, download its “fix,” or follow instructions to paste commands. Close the tab or browser. If it will not close, get trusted help. Seeing a warning alone does not prove the device was compromised.

Remote control can expose far more than a screen

Remote access can let someone open files, read email, view financial information, install software, or change settings. Some tools can be configured to reconnect later. Ending a call does not necessarily remove that access.

Never give an unverified stranger remote access.
A legitimate remote-support program can still be used by a criminal.

Only allow a session you arranged with a verified, trusted provider. Stay present, understand the work, and end access afterward. Do not sign in to banking or payment accounts while someone controls or watches the device. A technician does not need your banking password or login code.

Sources: FTC tech support scams; Microsoft support-scam guidance; HP Fraud Alert [9-11]. See the reference list on page 10.

5. Passwords and two-factor protection

Use a different strong password for every account

Reusing a password lets a breach at one company threaten other accounts. Avoid names, birthdays, phone numbers, common phrases, and predictable substitutions such as changing “a” to “@.”

Use a reputable password manager to generate and store a long random password for each site. Aim for at least 16 characters where allowed. A long passphrase made from randomly chosen unrelated words is another option; avoid famous quotations or personal facts.

No one can verify that nobody else on Earth has ever used a password. The practical goal is a password so long and random that duplication or guessing is extremely unlikely, and that **you never reuse**. Do not use example passwords printed in any guide.

Turn on two-factor authentication (2FA)

2FA adds another check beyond your password. Enable it on **email first**, because email often receives password-reset messages. Also enable it on banking, investments, credit cards, payment apps, shopping, travel, subscriptions, and any account with a saved card or other financial implications.

In each account's Security settings, look for “two-step verification,” “2FA,” or “multifactor authentication.” Where offered, choose a passkey or security key; an authenticator app is another strong option. Text-message codes are generally better than having no second factor.

Never read a login code to a caller or approve a sign-in you did not start. Scammers can trick people into bypassing 2FA.

Keep recovery codes somewhere secure and separate from the device. Protect your password manager with a strong unique master password and 2FA. Keep recovery contact details current; ask a trusted helper if setup is confusing.

Sources: FTC passwords and two-factor authentication; CISA password guidance [12-14]. See the reference list on page 10.

6. If a scammer gained access

Act promptly. You do not have to prove money was stolen before asking your bank for help.

• **1. Stop the connection.** End the call and remote session. Turn off Wi-Fi and unplug the network cable on the affected device. If you cannot disconnect it, shut it down. Do not reconnect it for email, banking, or password changes before it is assessed.

• **2. Contact your bank immediately.** From a trusted phone or device, call the number on your card or statement. Explain that someone had remote access, what accounts were open, and whether money or credentials were shared. Ask about protecting accounts, disputing charges, stopping transfers, and replacing cards. Recovery is not guaranteed.

• **3. Contact other affected providers.** Notify card issuers and payment services. Use a known-clean device to secure email and financial accounts. Change exposed or reused passwords, revoke unfamiliar sessions, and review recovery details, email forwarding rules, and 2FA settings.

• **4. Arrange a device inspection.** After contacting your financial institution, call Lemon Bay Computer Service at **(941) 548-1322**. Bring affected devices to our shop at **30 N Elm St, Englewood** for inspection and, if needed, removal of unwanted software or a more thorough system cleanup or reset.

Tell us what happened and which programs were installed. An inspection can help identify unauthorized access; a clean scan alone cannot guarantee that no information was copied. Device cleanup does not reverse stolen money or secure compromised online accounts by itself.

• **5. Preserve and report.** Keep messages, receipts, phone numbers, and a timeline without reopening suspicious links. Report at **ReportFraud.ftc.gov**. If personal identity information was exposed, use **IdentityTheft.gov** for a recovery plan.

Sources: FTC recovery guidance and tech support advice; Microsoft recovery guidance [9,15-16]. See the reference list on page 10.

7. Your everyday safety checklist

Before you click, call, or pay

• Did I expect this message or call?

• Is someone creating fear, urgency, or secrecy?

• Have I checked through an official app, saved website, or trusted phone number?

• Am I being asked for a password, login code, payment, or remote access?

• Have I paused and asked someone I trust?

Keep your protection current

• Use a unique, long password for every account and turn on 2FA wherever available.

• Install operating system, browser, app, and security updates. Use automatic updates when practical.

• Keep backups of important files. Check that you can restore them.

• Turn on bank transaction alerts and review statements. Ask the bank about a trusted contact where available.

• Do not give a second caller money to “recover” a scam loss. Recovery promises can be another scam.

Write down trusted contacts

My bank: _____
Trusted friend or family member: _____
Their phone: _____

Lemon Bay Computer Service
(941) 548-1322 | 30 N Elm St, Englewood
Call us if you are unsure. It is better to pause and check.

Tell your technician whether you clicked, downloaded software, shared information, or allowed remote access. The response should match what happened.

Sources: FTC passwords, recovery and scam guidance; CISA Secure Our World [8,12,15,17]. See the reference list on page 10.

References and trusted resources

Official consumer guidance used for this manual. Reviewed October 7, 2026. Website instructions can change. This manual provides general prevention and recovery guidance; it does not promise that any account or device is completely safe.

1. FTC: Recognize and avoid phishing
2. FTC: Spam text messages
3. Microsoft: Protect yourself from phishing
4. Meta: Account security
5. Meta: Avoid scams online
6. Meta: Anti-scam tools and account-linking scams
7. FTC: Phone scams
8. FTC: How to avoid a scam
9. FTC: Tech support scams
10. Microsoft: Technical support scams
11. HP: Fraud alert
12. FTC: Strong passwords
13. FTC: Two-factor authentication
14. CISA: Password tip sheet
15. FTC: What to do if you were scammed
16. Microsoft: Recover from a tech support scam
17. CISA: Secure Our World

In the digital PDF, select a reference title to open its source. For printed copies, start at consumer.ftc.gov, support.microsoft.com, support.hp.com, or facebook.com/help and search for the title.

Report fraud: ReportFraud.ftc.gov
Identity recovery: IdentityTheft.gov
Local device help: (941) 548-1322