4-H TECH CHANGEMAKERS

LESSON TITLE: COMMUNICATION: E-MAIL BASICS

Overview
E-mail is one of the most fundamental internet communication tools. E-mail is an electronic message that is sent from one person to another through digital messaging systems. E-mail saves both time and money compared to regular mail. An e-mail message literally takes no more than a few minutes to reach the receiver.

Objectives for Adult Learners:
After participating in this lesson, adult learners will be able to:

- Identify key e-mail communications platforms
- Explain the steps that must be completed to send an e-mail
- Protect oneself from e-mail malware

Objectives for 4-H Tech Changemakers:
Before teaching this lesson, the 4-H Tech Changemakers should be able to:

- Describe the process of sending an e-mail
- Demonstrate core and advanced e-mail communication skills
- Explain proper e-mail etiquette

It is recommended for 4-H Tech Changemakers to practice these skills multiple times (using different devices, if possible) before teaching any workshop sessions.

Materials & Supplies
The following materials and supplies are needed for this lesson:

- Digital devices and access to the Internet (activity 1, activity 2)
- Access to the Internet (activity 1, activity 2)
- Flip chart and markers (activity 3)
- Phishing examples (activity 4a)
- Report Phishing cards (activity 4b)

Preparation
In preparation for this lesson, facilitators should:

- Review lesson plan
- Ensure Internet connectivity at workshop location and check website links
- Gather all materials and supplies
- Copy any handouts, if needed

Lesson Implementation Ideas:
Depending on the teaching setting and amount of time you have, there are a variety of ways to implement these activities. Suggestions include:

DELIVERY MODE	Face-to-Face	Face-to-Face	Face-to-Face	Exhibit	Virtually
TIME	30 minutes	1 hour	2-part series	10-15 minutes	1 hour
SUGGESTED ACTIVITIES	Activity 2	Activities 1-3	Part 1: Activities 1-2 Part 2: Activities 3-4	Activity 2	Activities 1-3

COMMUNICATION: E-MAIL BASICS (CONT.)

Terminology:
The following terms will be discussed during the lesson:

- **E-mail:** messages distributed by electronic means from one computer user to one or more recipients via a network.
- **Malware:** software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Password:** a combination of keyboard letters, numbers, and characteristics that must be entered to gain admission into many online services (e-mail, social media accounts, online shopping accounts, etc.).
- **Phishing:** the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication.
- **Security Question:** form of shared secret used as an authenticator for accessing digital platforms and information.

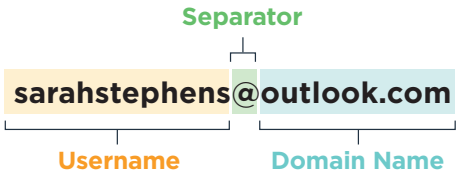
Background Information:
E-mail is one of the most fundamental internet communication tools. E-mail is an electronic message that is sent from one person to another through digital messaging systems. E-mail saves both time and money compared to regular mail. An e-mail message literally takes no more than a few minutes to reach the receiver. While sending e-mail can be efficient and cost-effective, it is important for digital safety and security to be considered. People may use e-mail for various reasons; examples include someone sharing their resume with a potential employer, an employer contacting a potential job candidate, sharing reports/files, etc.

E-mail features can vary based on the platform being used. However, generally all e-mail platforms can send e-mail (including attachments), reply/forward/reply all e-mails, sort/file e-mails, etc.

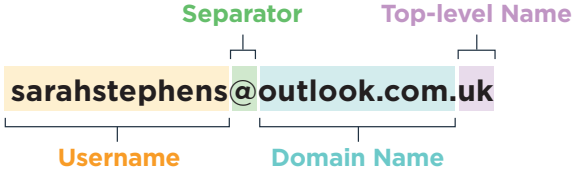
NOTE: *Remind participants to not share their password (even as an example) during this lesson.*

E-mail is an electronic message that is sent from one person to another through digital messaging systems. E-mail travels via the Internet from one computer to another. When we click on the send button in an email program the client connects to the Simple Mail Transfer Protocol (SMTP) server which then connects to the Mail Transfer Agent (MTA). The SMTP server is like the mail carrier who picks up your e-mail from your house and drops it off to the MTA. The MTA is like the post office and deposits the email in your post office box. For the MTA to deposit the mail though, it must ask the Domain Name System (DNS), which is like a global address book for the path of the domain name. The server at the domain name will then deposit the mail into the user mailbox. All of this happens in less than a couple of minutes.

Facilitators should write an example of an e-mail address on a flip chart. At the most fundamental level, e-mail addresses consist of three or four parts (1) username, (2) separator, (3) domain name, and the optional (4) top-level name.



1. Username (yellow): this is the 'name' of the e-mail account that is created by the owner. Many times, people use their name, parts of their name, and/or a combination of numbers to create their account name.
2. Separator (green): this is the "at" sign or symbol (@). When reading aloud, it's spoken as "at."
3. Domain Name (blue): this name identifies the server where the email messages are sent and stored.



4. Top-level Name (purple): this identified a country associated with the address. Sometimes this information is not included in an e-mail address.

There are two ways that people can be provided e-mail services. E-mail can be provided by an Internet Service Provider (ISP). People usually pay a monthly fee for internet connections, and many times, a free e-mail account can be provided. For example, BellSouth is an ISP and customers would have a domain name associated with this company (such as example@bellsouth.net). There are also free web-based e-mail service providers. Usually advertisements are associated with this site, so these companies pay for the advertisement which allows the user to have the service for free. For example, Outlook provides free e-mail services and users have a @outlook.com domain name.

There are two ways for people to check e-mail. Web-based e-mail (such as Hotmail) allows the user to login to a website to access the account. The e-mail messages stay on the mail server and can be accessed from any computer with Internet connection. E-mail software (such as Outlook) allows to user to login to the e-mail software application. The application retrieves your messages from the mail server and saves them to your computer's hard drive. There are some services (like Outlook) that also have web-based access, allowing users to be able to log in from any device to access their messages. However, these messages do not download to the computer's hard drive. To access e-mail, people will have to submit a password. Sometimes, an additional layer of security may be added. Participants may also have to answer a security question. These security questions might also be used when participants need to reset their password (usually when they forget their password).

NOTE: *Facilitators may choose to include some information from the Strong Passwords lesson plan.*

Facilitators should allow time for participants to explore their current e-mail account. If participants do not have an e-mail account, facilitators may choose to help them sign-up for an account. Remember that no participant should feel pressured to use an e-mail messaging system. Facilitators should also not learn personal information about the participants – password, security questions/answers, etc.

ACTIVITY 2: Using E-mail to Communicate

There are a variety of things you can do with an e-mail account:

- **Compose & send messages:** write a message and send to someone else
- **Reply:** respond back to an e-mail someone else sent to you
- **Forward:** pass along an e-mail you received from others
- **Attach:** send a file (such as a document or photo) to someone else by attaching it to a message

NOTE: *It is recommended to explain each of these different actions and then have facilitators work one-on-one with participants to show how to do these skills on their devices.*

Composing a Message: When starting a new e-mail, most services have a "compose" or "new" button. After clicking that button, the blank e-mail message appears. You will have to type in the e-mail address to the person who is receiving the message (just like you would write an address on an envelope). You will also have the ability to type a subject of the e-mail. The subject should be kept short but also be specific. For example, "hello" is a confusing subject while "Inquiring about Warehouse Job" is more specific. The e-mail program will automatically include the date/time sent as well as your e-mail address as the "sender" of the message.

In the body of the e-mail, you will have the ability to type the message. While you don't necessarily have to write as if it were a formal letter, most people include a greeting, body/text, a closing, and their name. People may also choose to include their contact information (such as a physical address or phone number). Usually this is associated with a business/work e-mail account. In the body of the e-mail, it is expected to use correct grammar, syntax, spelling, mechanics, etc. Many programs offer a free spell/grammar check program. When you are ready to send the message, click the 'send' button.

Replying to a Message: If you receive an e-mail message from someone, chances are, you will want to reply. This is like having a conversation. After reading the e-mail, you will click the 'reply' button and write a message back. When you are ready to send the message, click the 'send' button.

NOTE: *Facilitators should choose to explain the difference between the 'reply' feature (where the reply e-mail is only delivered to the original sender and the 'reply all' feature (where the reply e-mail is delivered to anyone who was sent the original e-mail).*

Forwarding to a Message: If you receive an e-mail message from someone and want to pass it along to someone else, you will want to click the 'forward' button and type in the e-mail address to the person who is going to receive the new e-mail.

Attaching an Item: If you want to send a file to someone (document, video clip, photo, etc.), the file must be attached to the e-mail. In order to attach a file, you must click the 'attach' button; sometimes it looks like a paper clip. After you click this button, you must find where the file is saved on your computer (My Documents, My Photos, Desktop, etc.) and click on the file's name to attach it. You can still send a message in the body of the e-mail with the attachment. When you send a physical letter in the mail, you can also include a photo in the envelope. Think of the original e-mail as a letter and the attached item as the photograph. When sending an e-mail with an attachment, you will still want to include a message in the body of the e-mail. For example, "Attached is my resume for job posting #104. Please let me know if you have any questions." could be included when a resume is being sent for an open job position.

Folders: Your e-mail account will have virtual folders. These folders help you organize your messages. Your inbox is where your incoming messages are stored. After reading them, you can choose to create your own folders (example – bills, banking, vacation, etc.) to file your e-mails. Any e-mail you send is saved in your 'sent' folder. After you delete an e-mail, it is in your 'deleted items' or 'trash' folder. To permanently delete the message, you must open this folder and delete the message again. (This is to prevent you from accidentally deleting a message.) Most e-mail services will also have a 'junk' or 'SPAM' folder. Usually the e-mail service can filer out unwanted/junk e-mails. (Some of these e-mails could be phishing attempts.) You should periodically check your junk folder to make sure any non-junk e-mails are not accidentally there.

Saving a Draft: If you have started writing a message and need to stop, you can save the message in your 'drafts' folder. When opening your e-mail again, the look in this folder and you will find your partially complete message.

NOTE: *It is recommended for facilitators to project an e-mail account and demonstrate these features live. You could also have facilitators work one-on-one with participants to show each of these actions (composing a message, replying to a message, etc.) within their own e-mail program.*

Recognizing Malware: Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Malware e-mails are typical, although many of today's e-mail systems help filter these e-mails using 'junk' or 'SPAM' folders.

NOTE: *Activity #4 focuses specifically on e-mail phishing attempts.*

ACTIVITY 3: Pros and Cons of E-mail Communication

Facilitators should lead a discussion about the pros and cons of using e-mail for communication. These can be listed on the flip chart. Facilitators may choose to share personal examples of how e-mail has been beneficial for them as well as any examples of how the have had negative experiences with e-mail. (The intent is to show how having an e-mail account is beneficial, so be cautious when sharing any 'cons'.)

The benefits of using e-mail include

- **Being fast** – messages are delivered in a short amount of time and can literally travel around the world
- **Response** – you can think-through a response and make any changes. When having a conversation (either in-person or on the phone), you don't have a chance to change your words.
- **Time** – the senders/receives of the message don't have to be working at the same time or place. Unlike a scheduled meeting, people can respond to e-mails as their schedule allows.
- **Record** – you have saved copies of e-mail your sent, so it's a great way to keep records of your communication.
- **Multiple People** – if you need send a message to a lot of people at once, e-mail makes it easy to do.

Some reasons you may not want to use e-mail include

- **Junk** – sometimes you can get junk/unwanted e-mails.
- **Ads** – sometimes advertisements can be included in messages.
- **Misinterpretation** – sometimes it is hard to infer tone/feelings through an e-mail
- **Forwards** – e-mail messages can be passed on to others. You should always count on the possibility of your message ending up in the inbox of someone it wasn't intended for.

Don't use e-mail for

- Long or complicated messages.
- Questions that require a lot of clarification.
- Delivering indiscreet, sensitive, or private information.
- Angry messages.
- Things you should say in person.

ACTIVITY 4a: Recognizing E-mail Phishing Attempts

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication. Distribute examples of a phishing e-mail and a phishing text.

Explain the following for the e-mail message:

The employee (who works for the University of Georgia) received this e-mail message. Her supervisor is Arch Smith, so she regularly receives e-mails from him. However, after further investigation, there are some suspicious things about this message:

- While the e-mail is from "Arch Smith," the sent e-mail address does not indicate that Arch sent the message. Since the correspondence is related to work, it's also suspicious that it did not come from an e-mail account associated with the University of Georgia.
- The spelling, grammar, and mechanics of the e-mail raise concerns. Words are capitalized that should not be. Punctation and grammar are incorrect in some instances.
- The e-mail isn't actually signed from Arch Smith. Most e-mails end with some sort of closing and signature.
- The e-mail seems very urgent and does not specifically cite why things are urgent. The sender also is not able to take phone calls (which would probably be considered a 'normal' practice in an emergency situation).

Explain the following for the text message:

The person banks with Wells Fargo and sometimes gets e-mail updates from the bank. However, after further investigation, there are some suspicious things about this message:

- The sender of this message uses the e-mail address customersatmbankingwells432@masbadar.com. It does not appear to be a legitimate e-mail address associated with Wells Fargo.
- The link embedded in the message is a bitly URL. Bitly is a service that shortens URLs – not showing the complete website URL. While many groups use these services, you should only click on the shortened URL when you know the sender.
- The spelling, grammar, and mechanics of the text raise concerns. The message is not complete.

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication. Phishing typically happens over e-mail. Many times, people that reply to these types of e-mails are asked to do something that does not keep them safe online. They may also be asked to click on a link and share information. For example, they may be asked to share their password, financial information, pin codes, or asked to send money or buy items (such as gift cards). Many times, timing is urgent because "suspicious activity has been detected" or "your account is locked" until further actions. This is simply not true.

Some features of a phishing e-mail include:

- Needing to verify account information (ex. e-mail account, banking account, money transfer account, etc.). Many times, the e-mail says your personal information has expired or needs to be verified.
- Link in the e-mail/text or attachment. Usually, the link does not provide you with the URL, so it's hard to determine what website it will redirect you to. Regardless, only click on links from reputable senders.
- Sense of urgency. Many times, phishing e-mails give you a limited amount of time (ex. 24 hours) to resolve a "problem" that doesn't exist.
- Too good to be true. Phishing e-mails could promise some sort of "return" such as cash or gift cards if you do something first (usually giving them personal/sensitive information).
- Spelling, grammar, and/or mechanics errors. An occasional typo sometimes happens in a legitimate e-mail, but an excessive amount of errors includes a phishing e-mail.
- Length. Some phishing e-mails can tend to be short. Others may be very long, explaining a circumstance (ex. why this person can't do something and why they need your help).
- Generic greeting. Many phishing e-mails don't have a greeting or simply start with 'hello.'

ACTIVITY 4b: Dealing with Phishing Attempts

Why is it important to avoid phishing attempts? During the summer of 2019, a metro Atlanta city was scammed out of $800,000 because of phishing. A city employee thought they got an e-mail from a vendor with the water department, but the e-mail was from a cybercriminal instead. The e-mail said the vendor was updating/changing their banking account, so they needed to verify all their customer's records. The city employee sent over the city's banking information, and the cybercriminal was able to transfer nearly $800,000 from the account before someone realized the mistake. While the city does have insurance and the scam was reported to authorities, it is unlikely all of the money can be recovered. While this example applies to a city, anyone can be a victim of a phishing attempt.

If you think are you experiencing a phishing attempt, you should ...

- Not clicking on any links or downloading any attachments. They might contain viruses or spyware.
- Not reply to the e-mail or text message.

- Mark/categorize the e-mail as "junk" or "spam".
- If the e-mail references an account and you are concerned about that account, call the company. However, do not use any of the contact information in the e-mail or text. Many times, these criminals create fake phone numbers. Verify the company's contact information elsewhere first (printed bill, verified website, etc.)
- Report the phishing e-mail to officials.

Phishing emails can be sent to the Federal Trade Commission (FTC) at spam@uce.gov and to the Anti-Phishing Working Group at reportphishing@apwg.org. Phishing attempts can be reported to the FTC at FTC.gov/complaint. Phishing text messages should be sent to 7726 (SPAM).

Reflection:
While the intent is to build e-mail communication skills, the facilitator needs to lead a debrief discussion at the end of the lesson. Potential debrief questions could include:

- How can e-mail communication be used in different careers?
- How can you use e-mail communication to connect with others?
- What are some of the important e-mail communication skills to have?
- What are some considerations to remember for e-mail communication etiquette?

Connection to LinkedIn Learning:

- **Learning Outlook 2016:**
  - » Get started with Microsoft Outlook 2016. This fast-paced, beginner-level course will help new users set up and use Outlook on Windows. Jess Stratton shows how to set up Outlook email accounts, read and organize mail, compose new emails, work with attachments, and handle junk mail. The course also covers creating new contacts and using the calendar.
  - » Duration: 48 minutes
  - » Level: Beginner

LinkedIn Learning

- **Gmail Essential Training:**
  - » In this course, author Jess Stratton takes you on a deep dive into Gmail, the free email service from Google. Jess starts with an exploration of the interface and the basics of how to compose, send, and reply to email. She covers staying organized by using labels, working faster by utilizing keyboard shortcuts, and adding additional email accounts. Jess walks through the text and video chat features in Gmail and how to access them quickly, as well as how to use Gmail offline and on a mobile device. She also shows advanced features including using operators to search, creating filters to automatically process messages, working with multiple messages, creating email groups with labels, and more.
  - » Duration: 1 hour, 35 minutes
  - » Level: Beginner + Intermediate

LinkedIn Learning

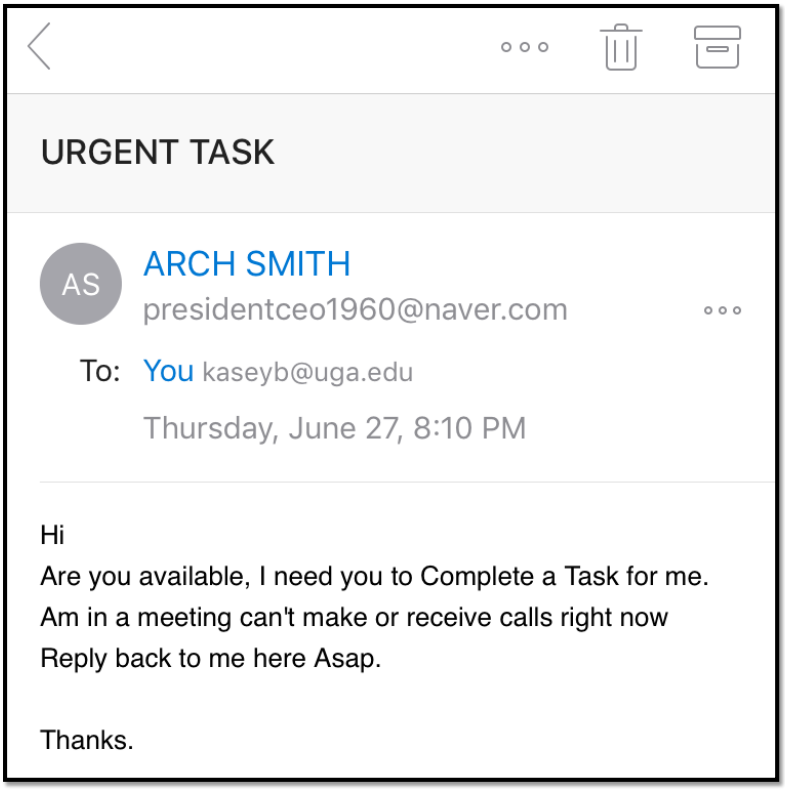
COMMUNICATION: E-MAIL BASICS (CONT.)

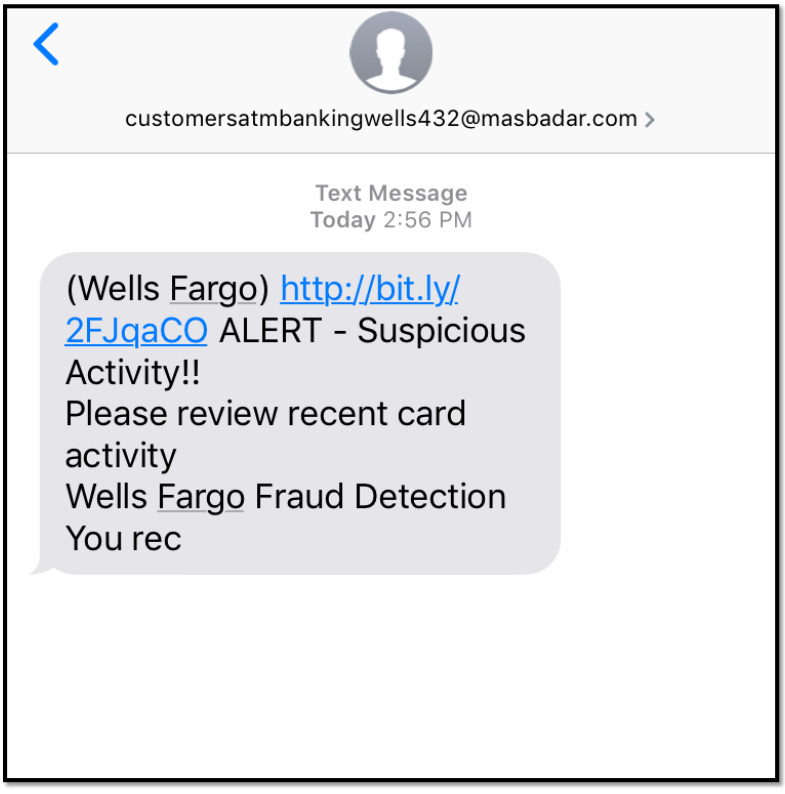
- **Writing E-mails People Want to Read:**
  - » In this course, instructor Sam Bennett shows you how to write great emails that'll leave a positive impression. First, Sam explains that being both personal and direct contributes to a high ROI, no matter who your recipient is. She goes over how to utilize the basic types of emails: inquiry, transactional or informational, and marketing or sales. She steps you through how to write engaging yet clear emails that grab your customer's attention and keep it. Sam teaches you what makes a good story work and what will convert prospects to customers. She walks you through best practices to make sure your emails get read at the right time by the right people and how to craft a relevant call to action. She shows you how you can reuse emails as blog posts, social media posts, and even compiled as ebooks. Sam concludes by discussing how to leverage email content to improve your FAQ and About US pages.
  - » Duration: 57 minutes
  - » Level: Beginner

- **Avoiding Phishing Scams:**
  - » It's easy to fall prey to phishing scams—even for the most tech-savvy computer user. In this short course, staff instructor Jess Stratton shows how to recognize the signs of a potential phishing scam to keep your computer safe from malicious attacks. Jess takes you through several email phishing scams, explaining how to look critically at the emails you receive. She points out some of the most common scenarios used by hackers—along with other telltale signs of a phishing email—so that you can protect your computer from email phishing scams.
  - » Duration: 6 minutes, 56 seconds
  - » Level: Beginner

Phishing Attempt Examples

To be used with E-mail Communication, Activity 4a





Report Phishing Cards

To be used with E-mail Communication, Activity 4b

Report Phishing!

Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.

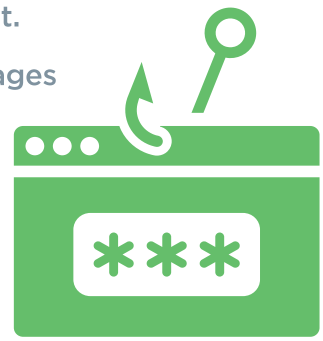
Report Phishing!

Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.



Report Phishing!

Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.

Report Phishing!

Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.