



FCC CYBERSECURITY AWARENESS TRAINING (CSAT)



This computer-based training presentation will take approximately 35 minutes to complete. Users are able to pause and resume the presentation, (from the last slide viewed, vice re-starting the entire presentation) as often as necessary.

Course Objectives

At the end of this course, you will be able to:

- Know Why Cybersecurity is Vital
- Know Legal Requirements
- Understand how to protect FCC sensitive information and IT assets and your personal data.
- Define privacy and personally identifiable information (PII)
- Identify Social Engineering and how the hackers are using it
- Recognize threats to information systems and privacy
- Know how to report a suspected or confirmed security or privacy incident.



Lesson 1

Cybersecurity Overview & FCC Security Policies





- Cybersecurity is **everyone's** responsibility. You have been assigned responsibilities ensuring information systems operate at an acceptable level of risk while supporting business operations.
- The cybersecurity team is ready to support you in complying with information security and privacy requirements.



Legal and Compliance Requirements

As an FCC employee, you are required to comply with a number of federal laws and regulations, as well as FCC internal policies and standards. This course focuses on the annual training requirements mandated by the following:

- The Federal Information Security Modernization Act (FISMA) of 2014
- Computer Fraud and Abuse Act of 1986
- Privacy Act of 1974, as amended
- Office of Management and Budget (OMB) Memoranda/Circulars
- NIST [Special Publication 800 series](#)



FCC Cybersecurity Program

- The Office of the Chief Information Officer (OCIO) has developed policies and procedures to help protect FCC's information and information systems:
 - The **FCC Cybersecurity and Privacy Program**- Provides direction on an IT security program and how to effectively safeguard FCC assets.
 - The **FCC IT Security Awareness and Training Policy** - Ensures annual security awareness and privacy training.
 - **FCC IT and Privacy Rules of Behavior (ROB)** - Provides the rules that govern appropriate use of FCC information resources and assets.

FCC Assets are anything of value to the FCC this includes but is not limited to information, hardware, software, and personnel.



Internet Safety and Email

E-mail use must not adversely affect performance of your role or reflect poorly on your organization. The following are FCC's terms of use for email as instructed in the **FCC IT and Privacy Rules of Behavior (ROB)**.

- Use only Microsoft Outlook as your official email client.
- Do not use personal emails to conduct FCC work/business.
- Refrain from opening suspicious emails and clicking on suspicious links within an email. Delete email from unknown senders.
- Check or verify the sender is from a known or trusted source.
- Avoid using "Reply All" to prevent sending unnecessary e-mail traffic.
- Do not send chain letters, jokes, offensive letters, mass email, unnecessary pictures.

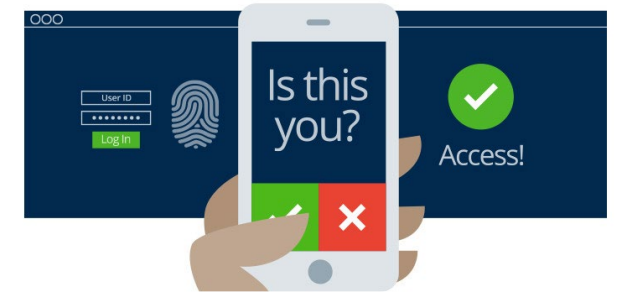
If you suspect an email is spam, **"REPORT" THE MESSAGE USING OUTLOOK OR O365 OR FORWARD** the email to Phishing@fcc.gov and then delete it from your Inbox.



Identity Management

Multifactor Authentication (MFA) uses more than one type of credential to verify your identity:

- Something you have, such as a Personal Identity Verification (PIV)
- Something you know, such as your Personal Identification Number (PIN)
- Something you are, such as a fingerprint or other biometrics



FCC currently uses three different options of MFA for strong network authentication and authorization.

- PIV card and your unique PIN
- RSA SecurID tokens and your FCC username/password
- Okta with your FCC username/password and Okta Verify mobile app



PIV Card Use and Protection

FCC PIV card grants employees' access to FCC facilities, and (together with your PIN) the FCC network and applications.



Use of PIV cards offers several benefits:

- Easier access to VDI
- No additional tokens or passwords
- No more passwords to remember, type and change, just a PIN that does not change
- One less thing to remember
- Allows for digital signatures and digital encryption



PIV Card Use and Protection (continued)

To protect your PIV card:

- Always maintain possession of your PIV card by removing and taking it when leaving your workstation
- Never surrender or exchange it for building access (e.g., a visitor pass)
- Do not write down or share the PIN
- Avoid using your PIV card as a form of photo identification for verification by a commercial entity
- If your PIV card is lost or misplaced, report it immediately to the FCC Security Office (SOC) at SOC@fcc.gov



Managing Passwords

A strong password should:

- Not be easy to guess
- Include a combination of 12 or more characters; at least 1 upper-case letter; at least 1 number, and at least 1 special character (s) like: "(space)!"#\$%&'()*+,-./:;<?@.
- Bad password (8): P@ssw0rd
- Great password (25): MysonwasbornNovember1995!
- Do not use personal information or common phrases
- Use Passphrases like: "I love my piano" = !Lov3MyPian0.



Password Tips

- Keep your passwords in a secure location
- NEVER share your password with anyone.
- Do not write down your password – memorize it
- Use Auto-generated passwords, near impossible to guess
- Separate passwords between systems or applications
- If you suspect your password is compromised, change it immediately and report the compromised password as an incident.



Remote Work Policies

You are responsible to protect FCC information whether you are at an FCC facility or at your dining room table.

- You should only access an FCC computer resource using an approved remote access solution:
 - VMWare Horizon Client (VDI)
 - Microsoft 365
 - FCC issued computer for remote use
- If using your personal computer to access FCC computer resources, make sure your software receives current updates and your antivirus is running.
- Only store FCC or any other Federal information in the FCC network (i.e., Box, OneDrive, SharePoint Online).
- Do not store or backup FCC data on personal removable media devices (e.g., USB Flash Drives, thumb drives, external hard drives, etc.)
- Use of publicly available devices or wireless connections (e.g., Internet kiosks in airports, hotels, libraries etc.) are highly discouraged due to high risk of compromise.



Best Practices for Personal Cloud Use

- Avoid storing sensitive information, including Social Security Numbers and bank statements, in the cloud
- If you must store sensitive information, encrypt it before uploading.
- Regularly back-up data in a separate and secure location.
- Use complex passwords or passphrases and enable MFA
- Regularly update software, operating systems, and anti-virus solutions, enabling auto-updates when available.
- If cloud account compromise is suspected, immediately change your passwords and security verifications.
- Enable security features for patches and updates on smart devices such as Amazon Alexa, Google Home, Apple Watch and Ring doorbells.



Best Practices for Social Media



- Understand and use the site privacy settings
- Create strong passwords or passphrases
- Don't give away your position through GPS or location links
- Avoid posting personally identifiable information (PII)
- Don't speak or appear to speak for FCC or post any embarrassing material
- If posting pictures of yourself in a work-setting, make sure there are no identifiable landmarks or items visible
- When establishing personal social networking accounts, never use your FCC contact information.



Physical Security Tips

- Remove your security badge after leaving your controlled area or office building
- Don't allow others access or to piggyback
- Don't talk about work outside your workspace
- Be careful when discussing sensitive information, such as PII, as people without a need-to-know may be present
- Be aware of people eavesdropping when retrieving messages from smartphones or other media
- Reporting suspicious activity to [FCC NSOC at NSOC-Monitor@fcc.gov](mailto:NSOC-Monitor@fcc.gov)



Lesson 2

Information Security & Privacy



Information Security & Privacy

The FCC has numerous technical tools to protect FCC data, including personally identifiable information (PII), but YOU play a critical part in safeguarding the information we handle.

This section of the training will explain what PII is, your responsibilities under the Privacy Act, what a breach is, and what to do when there is a breach.



Privacy: Why Do I Care?



In order to do business with the Federal Government, individuals often must provide personally identifiable information (PII) to agencies. Individuals reasonably expect agencies to protect PII, because, among other things, the unauthorized use or disclosure of such information creates a risk of identity theft or other harm to submitting individuals.



Under the Privacy Act of 1974 and other federal requirements, all FCC employees, contractors, and others (e.g., USAC employees) who handle PII on behalf of the FCC must safeguard it.



The Privacy Act contains civil and criminal penalties, including fines, if someone knowingly and willfully violates the Privacy Act.



Privacy: When Do I Need To Think About It?



You have an ongoing obligation to protect the PII that the FCC collects, maintains, and processes. But there are specific situations when you should be especially mindful of privacy concerns.



When standing up a new FCC program that involves the collection, maintenance, processing, or disclosure of PII, you should make sure to limit the information to what is necessary.



When creating or acquiring a new information system that will collect, maintain, process, or disclose PII, you will be required to go through an authorization process that assesses privacy risks.



When modifying an FCC program or information system with respect to what PII is being collected, how it is being used, or to whom it is being disclosed, you must go through similar processes.



When responding to a request to share PII outside of the FCC, including via publication or with third parties, the disclosure must be authorized, and protections must be in place.



PII: Business Contact & Certification Information

62554

Federal Register / Vol. 87, No. 165 / Friday, August 26, 2022 / Notices

FEDERAL COMMUNICATIONS COMMISSION

[FR ID: 101751]

Privacy Act of 1974; System of Records

AGENCY: Federal Communications Commission.

ACTION: Notice of a modified system of records.

SUMMARY: The Federal Communications Commission (FCC, Commission, or Agency) proposes to modify an existing system of records, FCC-2, Business Contacts and Certifications, subject to the Privacy Act of 1974, as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of records maintained by the Agency. The Commission uses the information on

PURPOSES OF THE SYSTEM:

The FCC and organizations administering programs on behalf of the FCC use this system to collect and maintain points of contact at entities regulated by the FCC and in related industries, as well as contractors, vendors, and those performing collateral duties for the FCC, to ensure compliance with applicable Federal laws and FCC rules, including through certifications of information provided to the Commission. The FCC also uses this system to collect and maintain contact information and certifications from other Federal, state, local, U.S. territorial, and Tribal government entities that administer, support, participate in, or receive information related to, FCC programs and activities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals, including points of contact for and those who certify on behalf of, businesses as well as Federal, state, local, U.S. territorial, or Tribal governmental entities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Contact information, such as name, username, signature, phone numbers, emails, and addresses, as well as work and educational history.

- Based on a review of its systems, evolving case law, and changed business practices, the FCC has determined that it should treat business contact and certification information as PII, subject to an agency-wide System of Records Notice (SORN), FCC-2.
- As explained below, this determination does NOT mean that you can no longer collect, process, or disclose business contact and certification information as part of an FCC program.
- This determination **DOES** mean that you should review the collection, processing, and disclosure of business contact and certification information to ensure that those practices are consistent with FCC-2.
- The Privacy Team is happy to work with you if you have any questions about what this determination means for your programs/activities.



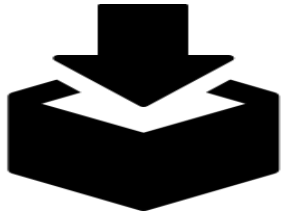
PII: Social Security Numbers (SSNs)



- Federal agencies are required under applicable OMB guidance to take steps to eliminate unnecessary collection, maintenance, and processing of Social Security Numbers (SSNs) and explore alternatives to the use of SSNs as personal identifiers.
- While limiting the collection, maintenance, and processing to the last four digits of SSNs is a helpful step, it does NOT eliminate the privacy risks to individuals.
- FCC policy generally limits the collection and processing of SSNs to instances where such collection and use are required by statute (e.g., Debt Collection Improvement Act), Commission regulations, other federal agencies, or courts with applicable jurisdiction.
- Under revised Privacy Team procedures, if your information system collects, maintains, or processes SSNs, going forward, you will need to annually justify the continuing need to do so.



Safeguarding PII



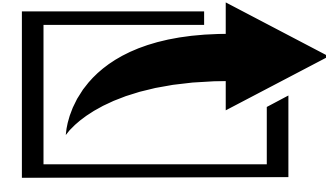
Collect

- Contact the OGC [Privacy Team](#), to ensure that (1) you have the legal authority to collect PII and (2) all the proper documentation is in place.
- Limit the PII you collect to only that information you need and use PII only for the purpose it was collected. If you want to use it for something else, talk to the [Privacy Team](#).



Maintain

- Do not leave PII unattended on desks, printers, fax machines, or copiers.
- Secure PII in a locked desk drawer or file cabinet, or similar locked enclosure whether you are working from an FCC facility or remotely.
- Only store PII on the FCC Network.
- Lock your computer when you walk away.



Disclose

- Confirm the disclosure is legally permissible.
- Ask whether an information sharing agreement or MOU is necessary or advisable.
- Wherever possible, share PII using OneDrive or Box. Email is not recommended.
- **NEVER** send it to a personal email address or store on your home computer.



Incidents and Breaches

Incident: An occurrence that:

- Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information or an information security system, or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.



PII Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where—

- A person other than an authorized user accesses or potentially accesses PII; or
- An authorized user accesses or potentially accesses PII for an other than authorized purpose.

Key Concepts:

- A breach occurs even if unauthorized access to PII is only “potential[]”; there is no need to wait to confirm that such access has occurred in fact.
- A breach does not happen only when a system is hacked; a breach occurs when an email containing PII is sent to the wrong recipient.



Reporting a Breach

- If you suspect a breach, immediately report it to the Network Security Operations Center (NSOC) at NSOC-Monitor@FCC.gov
- Do NOT wait to investigate. A delay in reporting the possible breach may allow more PII to be compromised.
- In your email, explain what happened (e.g., misdirected email, missing papers), who was involved (e.g., recipient of misdirected email), when it happened and when it was discovered, what PII was involved, and how to contact you.



Lesson 3

Cyber Threats & Social Engineering



Cyber Crimes

Cyber threats and vulnerabilities put information assets at risk. **You are the first line of defense in mitigating a potential threat.**

- **Threats** are the potential to cause unauthorized disclosure, change, or destruction to an asset. It can adversely impact FCC's operations, assets, other organizations, individuals, or even the Nation.
- **Vulnerabilities** include any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
- **Risk** is the likelihood that a threat will exploit a vulnerability.



Cyber Attacks

What is meant by “Attack”

Attacks on information security can be defined as an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm.

Types of Tactics Used in Cyber Attacks

- Social Engineering
- Malware
- Ransomware



Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system to obtain your personal information, access sensitive government information, and even steal your identity.

Examples are:

- Phishing
- Spear phishing
- CEO Fraud (BEC -business email compromise)

Since about 91% of data breaches come from phishing scams, this has become the most common type of social engineering.



Phishing Attacks

Phishing is when criminals use fake emails, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment.

- If you click on a phishing link or file, you can hand over your personal information to the cybercriminals.
- A phishing scheme can also install malware onto your device.
- E-mails or pop-up messages may appear to be from a legitimate source such as FCC your bank or family member.
- They will often contain the organization's logo and trademark. The URL in the email resembles the authentic web address.



It's Important to Hover before you click !



Why Hover?

Hovering over the links would be a dead giveaway that this is a phishing email, but enough targeted users click without thinking and scams like this continue.

- Blue text can be deceiving
- Underlying URL may be different
- Numbers instead of letters
 - Example: 192.168.1.1
 - Don't trust it!
- Any doubts? Don't click it!!!

The screenshot shows an email header with the following text:

From: FCC Surveys info@fccsurvey.net
Sent: Wednesday, June 29, 2022 6:12 AM
To: FCC Cyber Security <CyberSecurity@fcc.gov>
Subject: [EXTERNAL]: Your Voice Matters! Survey

Annotations include:

- A box pointing to the email address: "Email address includes 'FCC' but is not from .gov"
- A box pointing to the subject line: "Caution Warning shown tells users email originated outside of FCC"
- A red-bordered box containing a caution message: "CAUTION: This email originated from outside of the Federal Communications Commission. Do not click on links or open attachments unless you recognize the sender and trust the content to be safe. If you suspect this is a phishing attempt, please use the 'Report Message' feature in Microsoft Outlook or forward the email to the NSOC."
- A box pointing to the link: "Hovering over link shows invalid url: http://fccsurvey.net/?rid=noto3id"

The email body contains the text: "Your Voice Matters! FCC Communications has shared the following item: [Click here for survey](#)"



Tips to identify a phish

- Unexpected email
- URL link misleading (e.g., www.gooogle.com)
- Bad grammar or misused words
- Generic or odd greeting (e.g., Hi Account User)
- Sense of panic or urgency
- Asks for your account, login information or payment
- Something just doesn't look right / Too good to be true
- Unrecognizable or unexpected attachment



Prevent Phishing Attacks

- Don't click links or download attachments unless you're confident of where they came from.
- Validate email is legitimate, type the URL of the retailer or other company into your web browser as opposed to clicking the link.
- Never provide your password, or personal or financial information
- Make sure your information is being encrypted. Indications that your information will be encrypted include a URL that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted.



- **DO "REPORT" THE MESSAGE USING OUTLOOK OR O365 OR FORWARD** the email to Phishing@fcc.gov and then delete it from your Inbox.



Malware

Malware (short for malicious software) does damage to, steals information from, or disrupts a computer system.

- Email links and attachments are two of the most common sources
- Some examples of malware are Ransomware, Viruses, Worms, and Trojan Horses

How to Combat malware

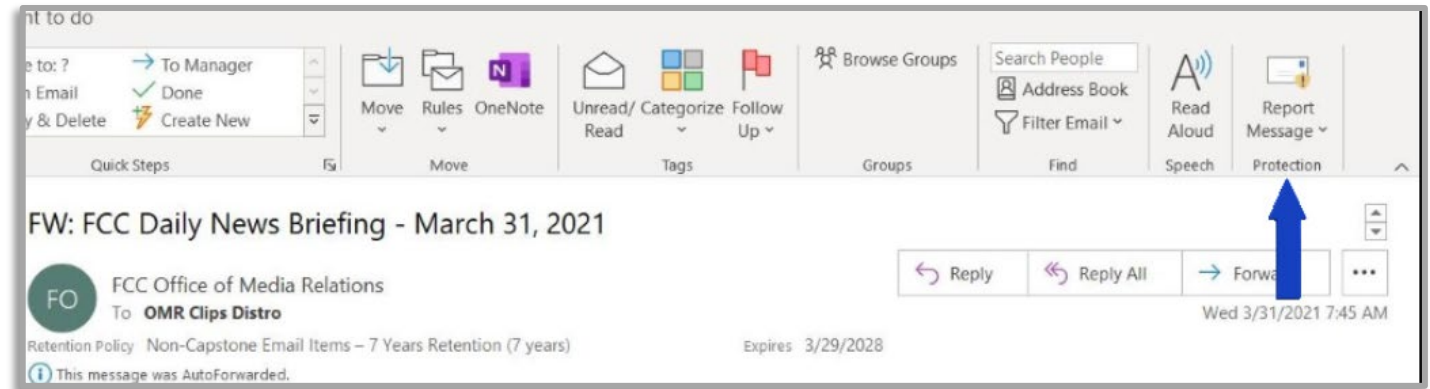
- Read email in plain text and do not use the preview pane
- Scan attachments with antivirus software before downloading
- Delete suspicious emails without opening them
- If you believe your computer is infected, immediately report suspected IT incidents to the NSOC at NSOC-Monitor@FCC.gov



Reporting Phishing Incidents - Inside VDI

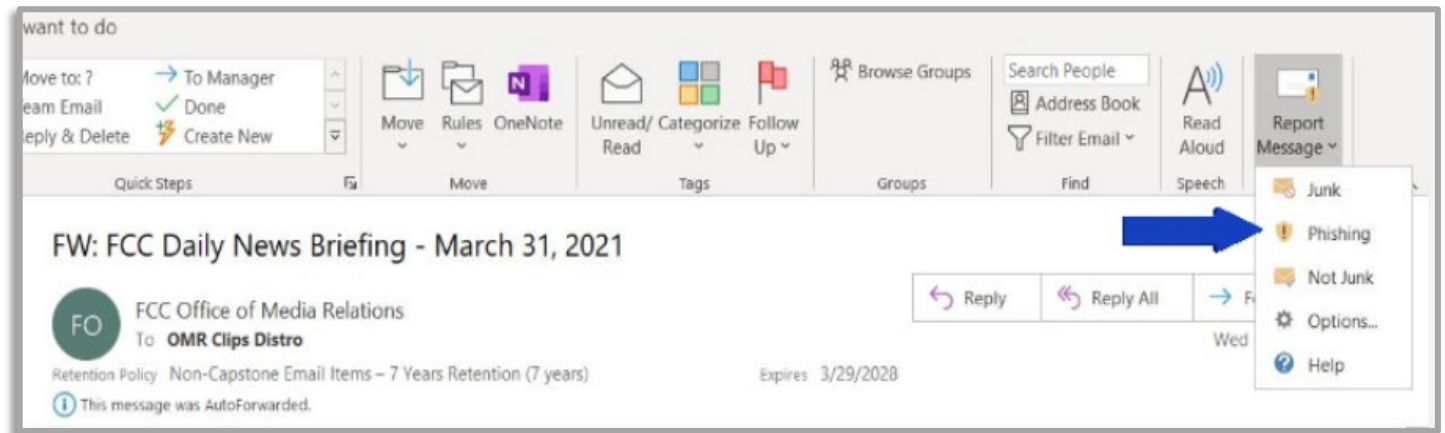
01

When working inside VDI in Outlook 365, you can report a Phishing attempt by clicking on “Report Message” in the toolbar.



02

Then select the “Phishing” icon to report the message to the FCC Phishing Team.



Reporting Phishing Incidents - Outside VDI

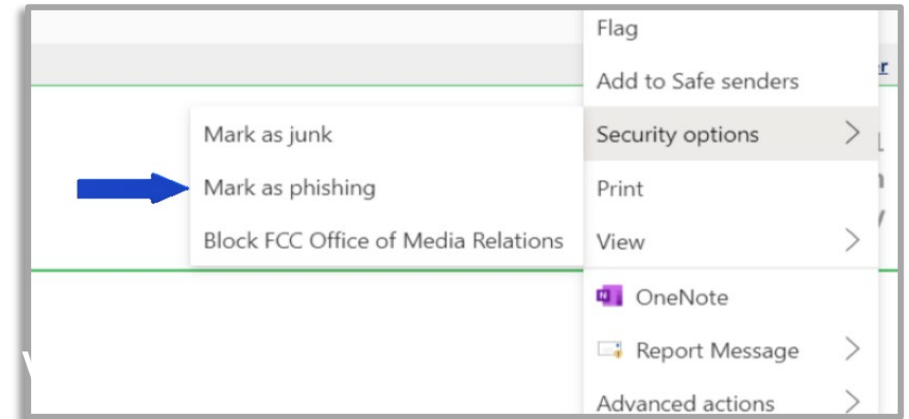
01

In the message reading pane, click on the 3 dots on the right in the ribbon.



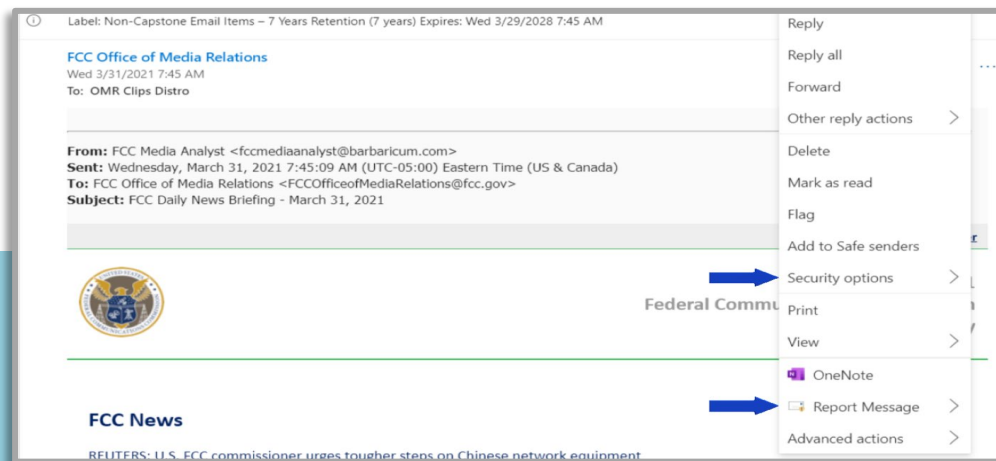
03

If you select Security Options, next click “Mark as Phishing” to report the message.



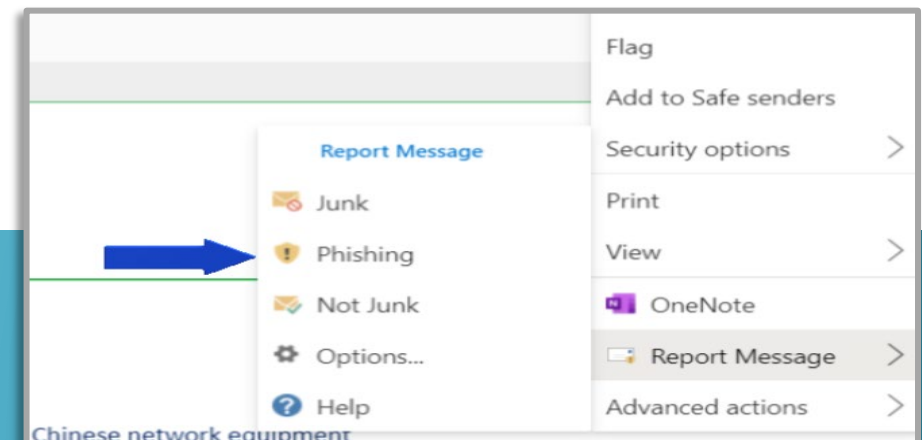
02

Click on either “security options” or “report message”.



04

If you select “Report Message”, next click on “Phishing” to report the message.



Reporting IT Incidents

Immediately report suspected IT incidents to the NSOC at NSOC-Monitor@fcc.gov

- Suspected Data breach or Malware
 - Privacy Breach
 - Unexplained system crash
 - Unexplained connection termination
- Provide a brief summary of the incident.
 - What occurred
 - Who was involved (if it affected multiple users)
 - When did the incident occur (date/time)
 - What application, network, or system was involved
 - Provide your contact information in the event the team requires additional information.
 - If it's a suspicious email, delete it from your inbox and "deleted items" folders.

Please note: Report all Phishing related Incidents to the FCC Phishing Team at Phishing@fcc.gov



Summary

The focus of this training was to raise the awareness of cybersecurity issues facing FCC. We presented an overview of the cybersecurity challenges that you encounter as a federal employee and provided you with the resources and tools to improve our cybersecurity posture through sound information technology practices.

Understanding how to protect FCC sensitive information is critical to ensuring the mission of FCC. By accepting your position in the Department and signing the Rules of Behavior, you accepted the responsibility to embrace the culture of cyber awareness, vigilance, and preparedness, and to immediately transform the practices you learned from this training into your daily work habits.



Congratulations

You have successfully completed the FY23 CSAT!

To receive your Certificate of Completion:

Please be sure to read the

“FCC Information Technology and Privacy Rules of Behavior (ROB)”
and then acknowledge that you have read, understand and agree to
comply with all stated guidelines and provisions.



Appendix A

REFERENCES AND ADDITIONAL RESOURCES



References

OMB Memorandum M-22-09, Federal Zero Trust Strategy

<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

Executive Order (EO) 14028 Improving the Nation's Cybersecurity

<https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>

FCC Directive 1479.6 FCC Cybersecurity and Privacy Program

<https://www.fcc.gov/sites/default/files/fcc-directive-1479.6.pdf>

FCC Policy for Cybersecurity and Privacy

<http://intranet.fcc.gov/docs/omd/itc/csp/notices/FCC%20Cybersecurity%20Program%20Cybersecurity%20Policy.pdf>

FCC IT Rules of Behavior (ROB): <http://intranet.fcc.gov/omd/it/security.php>.

Federal Information Security Modernization Act (FISMA) of 2014

<http://csrc.nist.gov/groups/SMA/fisma/faqs.html>



Additional Resources and Links

OPM 5 CFR Part 930, Subpart C.

<https://ecfr.io/Title-5/Section-930.301>

NIST SP 800-50, Building An Information Technology Security Awareness and Training Program:

<https://csrc.nist.gov/publications/detail/sp/800-50/final>

NIST SP 800-16, Information Technology Security Training Requirements: A Role-Based Model for Federal Information Technology / Cyber Security Training: <https://csrc.nist.gov/publications/detail/sp/800-16/final>

The Homeland Security Presidential Directive 12 (HSPD-12): <https://www.dhs.gov/homeland-security-presidential-directive-12>

Federal Trade Commission Fraud Reporting: <https://www.ftccomplaintassistant.gov/#crnt&panel1-1>

Cybersecurity and Infrastructure Security Agency: <https://us-cert.cisa.gov/ncas/tips>

Recent examples of Insider Threats: <https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches>




Clues:

1. Sense of urgency- fear tactics
2. Imitating known brand- fake email address
3. Impersonal
4. Urgency- punctuation and grammar mistakes
5. Rollover shows malicious link
6. Scare tactics
7. Impersonal- not real customer service
8. Copyright date is incorrect- location is incorrect
9. ZIP file

Phishing Example

- 1 **Payment Declined – Update Required Immediately!**
- 2 From: ApplePay Support customer_support_ref_@apple.com
- 3 Dear Apple User,
- 4 It has come to our attention that you're recent payment was declined. An update is required immediately..
- 5 To make this change, visit the support section at the link below.
<https://www.Applepay.com/subscriptions/payment-update>

http://944.535.32/index/apple.html
Ctrl+ Click to follow the link
- 6 If you do not update your payment information in the next 24 hours, your account will be deactivated.
- 7 Regards
ApplePay Support
- 8 Copyright©2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001
- 9  **apple-invoice.zip** [Download](#)