



**HRSA**  
**Healthy**  
**Grants**  
**WORKSHOP**  
Presented as a Web Series

**HRSA**  
Health Resources & Services Administration

# Cybersecurity for HRSA Award Recipients

Healthy Grants Workshop  
*August 13, 2025*

**Srinivas Panguluri**  
**Acting Chief Information Officer**  
Office of Information Technology (OIT)

**Vision: Healthy Communities, Healthy People**



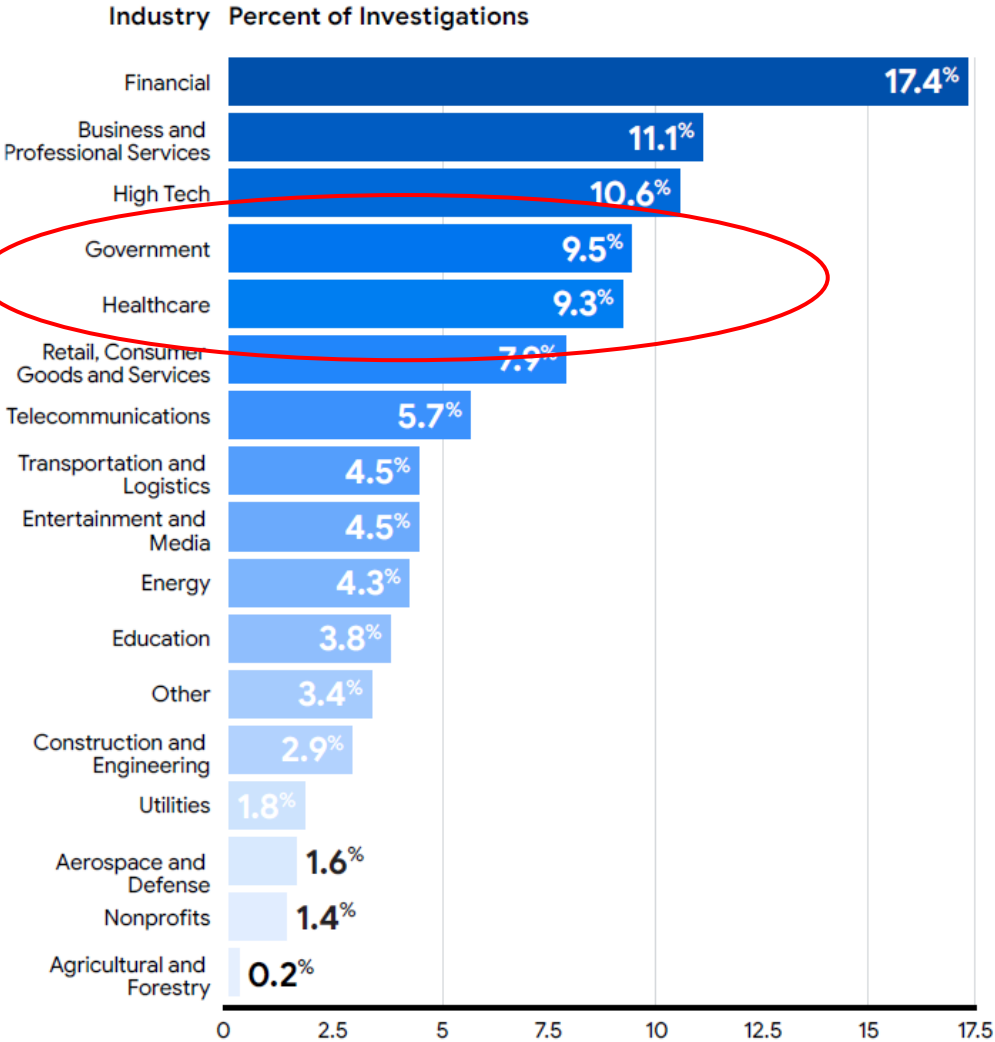
# Agenda

---

- Cyberattack Trends
- Top 10 Cyber Safety Tips
- Passwords and Multi-Factor Authentication (MFA)
- Phishing: Don't Get Hooked!
- Phishing: Examples #1 through #5
- Ransomware: A Growing Threat
- Artificial Intelligence is Transforming Cybersecurity
- Safe Browsing Habits
- What to Do if Something Goes Wrong

# Cyberattack Trends

Targeted Industries, 2024



Initial Infection Vector, 2024



Mandiant M-Trends 2025 Report (Google Cloud Security)

# Top 10 Cyber Safety Tips

---

1. Use strong, unique passwords or a password manager
2. Don't reuse passwords across different accounts
3. Turn on Multi-Factor Authentication (MFA) for key accounts
4. Think before you click (avoid suspicious links or attachments)
5. Limit what you share online (especially on social media)
6. Avoid public Wi-Fi for sensitive tasks (use a VPN if needed)
7. Keep software and devices updated (enable auto-updates)
8. Back up your data regularly (cloud + external drive)
9. Lock your devices with PINs, biometrics, or passcodes
10. Report suspicious activity

For more tips visit: [Secure Our World | CISA](#)

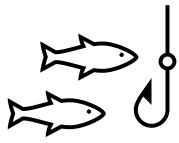


# Passwords and Multi-Factor Authentication (MFA)

---

- [NIST Special Publication 800-63B](#) - Digital Identity Guidelines
  - Passwords should be easy to remember and hard to guess, for example longer passphrases instead of complex characters (e.g., ThreeRedCatsDance!, Books&Blankets4Winter)
- MFA requires the use of **two or more** distinct authentication factors:
  - Something you know (e.g., password)
  - Something you have (e.g., mobile device – e.g., app based)
  - Something you are (e.g., fingerprint or face recognition)
- Phishing-resistant MFA: Smart Cards (PIV/CAC) and FIDO2 keys (YubiKey)






# Phishing: Don't Get Hooked


---

- **Phishing:** emails or text messages trying to hook you and steal information.
- **Clues:** urgent language, misspellings, strange links or attachments, or unusual sender.
- **Types:** Uniform Resource Locator (URL) phishing with embedded links (e.g., click here to unlock...), attachments, credential stealing (requiring data entry), QR codes, text message, etc.
- **Targets:** 1) spray and pray, 2) spear phishing - targets specific person, group or organization, 3) whaling – targets high ranking executives.
- **Methods:** They **target an emotion** to **motivate a response**. Generate a sense of curiosity, or fear, or urgency, or reward/recognition, or entertainment, or job opportunity, or social, etc.







# Phishing: HRSA Example #1

[EXTERNAL] Salary Account Update

 Jennifer Riggle <info@gherediaarquitectura.com>  
To: Devoss, Elizabeth (HRSA)

 If there are problems with how this message is displayed, click here to view it in a web browser.

The sender's address is impersonating a HRSA employee.

  Reply  Reply All  Forward  

Thu 11/16/2023 2:13 PM

---

Elizabeth,

I would like to update my account information on file before the next payroll is processed. What details do you need?

Best Regards,  
Jennifer  
Director, Division of Grants Policy  
Health Resources and Services Administration (HRSAgov), HHS

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and are confident the content is safe.



# Phishing: HRSA Example #2

Subject [Unknown] [EXTERNAL] Request #12/Sep/2023  
From [Unknown] ngewirtz@adleraphasiacenter.org  
(Health Resources And Services...)  
To EDeVoss@hrsa.gov  
Originating IP b224-59.smtp-out.eu-central-1.amazonaws.com (69.169.224.59)  
SMTP Relay nihxwaye3as04.hub.nih.gov (10.111.201.250)

## Microsoft E-Service Hrsa

### Password Expiration Notice

Hi **edevoss** , Your password for **edevoss@hrsa.gov** is set to expire  
on Tuesday-September-2023 19:32 PM EST.

Use same password with the button below

[Continue Same password Here](#)

← The sender is trying to get a HRSA employee's password.

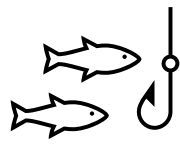
[Learn about messages protected by Office 365](#)

Microsoft respects your privacy to learn more, Please read our [privacy statement](#)

Microsoft Corporation, One Microsoft Way, Redmond WA 98054







# Phishing: HRSA Example #3

Subject: [EXTERNAL] Potential\_SPAM:New email 6542852  
From: lp0976411@gmail.com  
(Frances H. Chiodo)  
To: CGaney@hrsa.gov  
Originating IP: 216.155.152.209 (216.155.152.209)  
SMTP Relay: smtp.gmail.com (Unknown)

Dear cganey@hrsa.gov,

We sincerely appreciate your choice to shop with us! We're excited to inform you that we have successfully received your order and payment. Your order details are as follows:

**Order Number: 65840054**  
**Order Date: November 1, 2023**

Order Summary:

- **Product Name: Advanced PC Security**
- **Payment Method: Online**
- **Payment Status: Confirmed**
- **Amount: \$159.99**

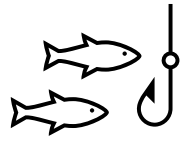
Please take a moment to review the order details above. If you happen to notice any discrepancies or have any questions, please don't hesitate to reach out to our dedicated customer support team by phone at **+1 805 434 6192**. We are here to assist you.

Thank you for choosing us for your security needs. We highly value your business and eagerly look forward to serving you. If you ever require any further assistance or have additional inquiries, please don't hesitate to get in touch with us.

Best regards,  
Frances H. Chiodo  
Toll-free Number: **+1 805 434 6192**

The sender is trying to get a HRSA employee to click on the link.





# Phishing: HRSA Example #4



Health Resources & Services Administration

2024 Health Resources & Services Administration 2022 Grant Information Verification.

The sender is impersonating HRSA.

Dear FAMILY VOICES OF NORTH DAKOTA, INC.

Kindly confirm if the below information about you is correct and up to date.

This is a final awareness for information verification.

Note: This secure verification link below will expire after 24 hours. We will have to revoke your license if we do not receive your

|   |                     |
|---|---------------------|
| Grantee Type Description                        | 118664817           |
| DUNS Number                                     | D132R56KXJK8        |
| Unique Entity Identifier                        | -98.713990949999996 |
| Geocoding Artifact Address Primary X Coordinate | 46.356898880000002  |
| Geocoding Artifact Address Primary Y Coordinate |                     |

The sender is using publicly available data to trick grantees.

Original URL:  
<https://dev.grants.hrsa.gov/pantheon.site.io/?email=fvnd@drtel.net>  
Click or tap to follow link.

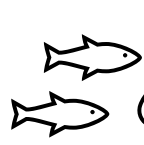
CLICK HERE TO VERIFY OR UPDATE YOUR INFORMATION.

This is a malicious link that will request name, email, phone number, SSN, driver's license.

al, and privileged, and is not to provide legal advice. Unless you are the intended addressee (or authorized to receive for the intended addressee), you on contained in the message without the sender's permission. If you have received this message in error, please advise the sender by reply email and

HHS Headquarters 200 Independence Avenue, S.W. Washington, D.C. 20201.





# Phishing: HRSA Example #5

Health Resources and Services Administration

Call or Text the Maternal Mental Health Hotline

HRSA  
Health Resources & Services Administration

Home Grants Loans & Scholarships

Verify your identity

Privacy Policy: Recipient's verification is required to access this page.

Email Address

Full Name

Active mobile number for verification

Social Security Number

Driver license front and back

Browse... No file selected. Upload clear front image of your driver license

Browse... No file selected. Upload clear back image of your driver license

Official verification

Browse... No file selected. Browse... No file selected.

Who We Are

The Health Resources and Services Administration is committed to providing equitable health care to the nation's underserved populations. We support people with low income, racial and ethnic minorities, parents, rural communities, transgender and gender non-conforming people, and people with disabilities.

This includes:

The sender is impersonating the HRSA web site.

The sender is trying to get the grantee to enter their email address.

The sender is trying to get the grantee to enter their name.

The sender is trying to get the grantee to enter their mobile number.

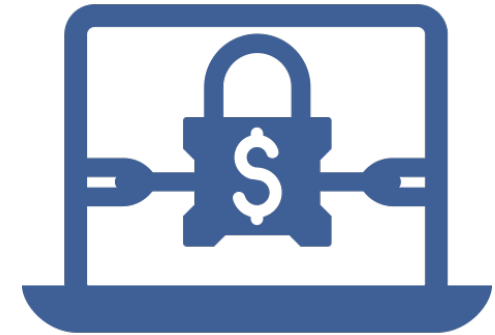
The sender is trying to get the grantee to enter their SSN.

The sender is trying to get the grantee to upload their driver's license.

# Ransomware: A Growing Threat

---

- Malicious software either encrypts your files or systems - making them unusable - or steals your data.
- The attackers then demand a ransom, often in cryptocurrency, either to prevent the stolen data from being leaked or to provide a decryption key to restore access.
- Average ransom payment: \$1.0 M; Average recovery cost \$1.5 M  
[2025 Ransomware Report: Sophos State of Ransomware](#)
- #1 cause: Exploited vulnerabilities - keep your system updated.
- Attacks often start via phishing emails or exploited vulnerabilities of unpatched systems.
- Prevention: Avoid suspicious links, report anything strange.




# AI is Transforming Cybersecurity

---

- AI is a double-edged sword in cybersecurity — a powerful defender and a growing threat.
- **Powerful Defender:**
  - AI can analyze billions of events to spot anomalies faster than humans e.g., detecting zero-day malware or insider threats
  - AI-driven automated response actions e.g., isolating infected machines in seconds
  - Machine learning (ML) to anticipate attack patterns before they occur e.g., flagging likely phishing domains based on behavior
- **Growing Threat:**
  - AI-Powered phishing, deepfakes and auto-generated emails increase realism and volume
  - Automated vulnerability scanning AI can help attackers find weak points faster
  - Adversarial AI attacks - cybercriminals can poison or deceive ML models

# Safe Browsing Habits

---

- Use HTTPS websites for secure communication (look for the padlock icon).
- Look at the URL and domain name carefully and use bookmarks. 
- Avoid downloading files or software from untrusted sources. If unsure, check URL and files:
  - ✓ VirusTotal (<https://www.virustotal.com>)
  - ✓ Google Safe Browsing (<https://transparencyreport.google.com/safe-browsing/search>)
  - ✓ URLVoid (<https://www.urlvoid.com>)
- Don't click on pop-ups or ads that seem too good or too alarming to be true.
- Avoid public and open Wi-Fi for sensitive transactions (e.g., banking).
- Mobile: Install apps only from official stores (Google Play, Apple App Store).



# What to Do if Something Goes Wrong

---

- The first few minutes after a ransomware attack are crucial. Swift isolation and notification can dramatically reduce damage. For example, disconnect device from the network, report it, and preserve evidence (e.g., don't reboot, but take pictures, etc.)
- Lost/stolen device or clicked on a suspicious link? Report to IT security staff immediately.
- Security is everyone's responsibility. See something weird? Speak up.
  - Unusual activity (e.g., password reset emails you didn't request).
- Report cyber incidents to your IT Staff and the HRSA Project Officer or the HRSA Contact Center as soon as possible.
  - HRSA can also take steps to take down the malicious site.





# Questions

---



# Connect with HRSA

Learn more about our agency at:

[www.HRSA.gov](http://www.HRSA.gov)



[Sign up for the HRSA eNews](#)

FOLLOW US:

