Cybersecurity
Protect Yourself & Your Voters

Secretary of State Staff
Dave Scanlan – Deputy Secretary of State
Tricia Piecuch – Assistant Secretary of State/Elections Director
Bud Fitch – Assistant Secretary of State/Election Legal Counsel
Colleen McCormack – Election Assistant
Debra Cornett - Director of Training
Phishing
Disinformation – RSA 659:40

• III (c) Attempting to induce another person to refrain from registering to vote or from voting at the proper place or time by providing information that he or she knows to be false or misleading about the date, time, place, or manner of the election.
  • It is your responsibility as election officials to know your voters and the election laws.
  • You need to instill confidence in the fairness and accuracy of our elections in your voters.
  • Example: You have a voter who comes into the office and states they just read on the internet that Republicans vote on Tuesday and Democrats vote on Wednesday.
    • How do you react?
Disinformation – RSA 659:40

- III (c) Attempting to induce another person to refrain from registering to vote or from voting at the proper place or time by providing information that he or she knows to be false or misleading about the date, time, place, or manner of the election.
  - How do you react?
  - Tell them who their Trusted Sources are:
    - Clerk – Election Official
    - SOS Office
    - Attorney General’s Office
  - Point the voter to the Voter Look-up Website to verify their polling place information.
Misinformation
An election official is listening to the news after getting home, the official hears an inaccurate result announced for their town; the news reports more votes cast in the official’s town for a candidate for an office than there were voters in their town.

What should the election official do?
Alert the clerk and moderator. The clerk or moderator should notify the media outlet with the correct information. By the next morning, notify the Attorney General and Secretary of State’s offices.
Entropy

`entropy` /ˈentrəpē/

**noun**
noun: entropy; plural noun: entropies; symbol: S

1. **PHYSICS**
   a thermodynamic quantity representing the unavailability of a system's thermal energy for conversion into mechanical work, often interpreted as the degree of disorder or randomness in the system.

2. lack of order or predictability; gradual decline into disorder.
   "a marketplace where entropy reigns supreme"

3. (in information theory) a logarithmic measure of the rate of transfer of information in a particular message or language.
An easy to remember pass phrase has a higher degree of entropy (is more difficult for the attacker to guess) than a complex, hard to remember password.
#1 – Do Not Open Attachments or Click on Links Unless You Know it is Legitimate and From Someone You Know and Trust

• If any question exists – call or e-mail the sender using a phone number/e-mail address from your records/\textbf{not} from the suspect e-mail.
#1 – Do Not Open Attachments or Click on Links Unless You Know it is Legitimate and From Someone You Know and Trust

- Example Below of real email sent to a supervisor of the checklist

```
medical card 12-07-2019

From: "Colleen McCormack-Lane <Colleen.McCormack-Lane@sos.nh.gov>" <auxiesorieria@gmpovid.com>
Date: 06 Dec, 2019 04:12PM
To:  

Hello,

Please find attached medical card.

I have enclosed a copy of the docs for your reference, you can download view using this link:

http://offers-istay.codingninjas.io/r3yavb1/available_array/test_portal/LzCL4wW_uH_Lm50LG77

Thank you

Colleen McCormack-Lane

Sent from my LG Mobil
```
Hover TO DISCOVER

Place your mouse/cursor over an email link and it will display the information contained in that link (hovering). Sometimes the type written words do not match the actual information contained in a link. By doing so you will see who the emailer actually is and/or where it will go.

If you are not sure:
- Contact the person or company directly
- Delete the email

![Email example with URLs and suspicious links highlighted]

![Hovering example with URLs and suspicious links highlighted]
Common feature of a phishing email to watch out for:

- They weren’t “expected” or “asked for” emails
- They are asking for money
- They often have a sense of urgency to them
- They try to trick you into clicking an incorrect link
- They try to steal login credentials by asking you to log in to a fake form
- They often threaten to disable your account or block an activity
- They may contain misspellings or bad grammar
- They seem very, or just a little, weird and/or unusual
#1 – Do Not Open Attachments or Click on Links Unless You Know it is Legitimate and From Someone You Know and Trust

• Just opening an attachment or clicking a link risks downloading malicious code, often in a process that will be invisible to you.
  • Ransomware – locks up your data, seeks a ransom payment
  • Malware – does damage to your files or computer software
  • Keystroke Recorder – captures and reports back your keystrokes, what you type into your computer – allows criminals to steal your usernames/passwords
  • Data theft – gain access to and steals private voter data or your office/person financial data.
#2 – Ransomware

- WHAT IS RANSOMWARE?
  Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.
#2 – Ransomware

HOW DO I PROTECT MY COMPUTER?

• Back up all important information, store offline and on a separate device (CD or Memory Stick)
• For ElectioNet data, the state has multiple levels of backups – your local responsibility is to save the checklist for your town regularly:
  • Before the election is entered into ElectioNet – save the Alpha List to a PDF file each month and after each supervisor’s session;
  • After the election is entered into ElectioNet – save the Checklist monthly and after each supervisor’s session
  • 4 weeks prior to the election save the checklist weekly
  • 2 weeks prior to the election save the checklist daily
• Store backups on a separate storage device.
#2 – Ransomware

**HOW DO I PROTECT MY COMPUTER?**

- Keep your software current – install windows and browser publishers updates as they become available.
- Install an anti-virus program sold by a major vendor
  - Avoid free or discount cost anti-virus programs.
  - Keep the anti-virus software updated.
  - Set the software to conduct regular scans of your system automatically.
- **NOTE:** January 14, 2020 Windows 7 operating system will no longer be supported.
  - We highly recommend you use Windows 10 or higher.
#2 – Ransomware

HOW DO I KNOW MY COMPUTER IS INFECTED?
Ransomware may direct a user to click on a link, through an email, to pay a ransom; however, the link may be malicious and could lead to additional malware infections. Some ransomware variants display intimidating messages, such as:
• “Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $10,0000 fine.”
• “You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently encrypted and no one will be able to recover them.”
WHAT TO DO IF INFECTED WITH RANSOMWARE?

• Isolate the infected computer immediately. Disconnect from any networks or attached storage devices.
• Power-off until an IT professional can assist with assessing the device.
• Have backups assessed to ensure they are not infected before using them to re-establish your files.
• Change all online account and network passwords using a different computer, not the infected computer.
• Notify law enforcement and the SOS Elections Division.
#3 – Cybersecurity Scenarios – What Would You Do?

On Election Morning you run the “Zero” tape on your ballot counting device and it shows “0” for most candidates and races, but has “27” votes for one candidate.  
- What would you Do?
#3 – Cybersecurity Scenarios – What Would You Do?
On Election Morning you run the “Zero” tape on your ballot counting device and it shows “0” for most candidates and races, but has “27” votes for one candidate.

- What would you Do?
1. Take the Ballot Counting Device out-of-service.
2. Deploy a ballot box and start the election using just the ballot box. Explain to all present that a certified device may be brought in and used to count ballots later during election day.
3. Provided the back-up memory card was successfully tested during the pre-election test, follow the vendor’s guidance in shutting down the device, disconnecting from power, replacing the memory card with the backup, then re-starting the device and running a new “Zero” tape.
4. If available, deploy a new Ballot Counting Device.
#3 – Cybersecurity Scenarios – What Would You Do?

On Election Morning you run the “Zero” tape on your ballot counting device and it shows “0” for most candidates and races, but has “27” votes for one candidate.

- What would you Do?

5. If available, arrange for the vendor to provide a replacement device.

6. Preserve the suspect memory card for the Attorney General’s Office.

7. Notify the Attorney General, Secretary of State, and your ballot counting device vendor.
#5 – Cybersecurity Scenarios – What Would You Do?

It is the Monday before election day. While you planned to print the checklists for the election last week, you ran out of time. You go to print the checklists and you cannot access ElectioNet. You contact the Help Desk and they advise that the system has suffered a cyberattack and IT staff is restoring the system. It is expected to become available later that day.

• What would you Do?
#5 – Cybersecurity Scenarios – What Would You Do?

It is the Monday before election day. While you planned to print the checklists for the election last week, you ran out of time. You go to print the checklists and you cannot access ElectioNet. You contact the Help Desk and they advise that the system has suffered a cyberattack and IT staff is restoring the system. It is expected to become available later that day.

• What would you Do?
1. Retrieve the PDF backup of the checklist you saved on Friday of last week and use it to print the checklist.
2. If a backup is unavailable, contact the Help Desk and request that the state’s backup copy of your checklist be sent/delivered to you.
Be confident in your New Hampshire Election

WE ARE A PAPER STATE

- Clerk has received their paper absentee and official ballots.
  - ✓ They have checked the paper ballots and confirmed the count.
- Checklist has been printed out on paper and certified by the Supervisors
- Moderators run the “zero” tapes to prove there are no votes for the candidates
  - ✓ Candidates are always listed as they appear on the ballot
  - ✓ Check for any anomalies on this tape
  - ✓ Check the tape again at the end of night with the final results
  - ✓ In a hand count town, before the first ballot is cast, the Moderator has opened and displayed the interior of the ballot box to all present, showing that the ballot box is empty.
- Could the grid (utilities) go down?
  - ✓ Most larger towns/cities have generators or we can always hand count the election.
Be confident in your New Hampshire Election

WE ARE A PAPER STATE

- Moderator fills out the ROV (Return of Votes) and it is transported by the NH State Police to the State House.
- Can the election night results reported by the press be wrong?
  - You disclose the tape results before adding in the hand count
  - You disclose results before discovering an error during reconciliation

✓ What numbers should the press/public rely on?
✓ You have 3 trusted sources:
  - Final Reconciled Numbers from Election Officials: Clerks, Moderators and Supervisors
  - Secretary of State’s Office
  - Attorney General’s Office

- A recount can always decide the winner.

You need to instill confidence in the fairness and accuracy of our elections in your voters.
Thank you!

If you have questions after today’s presentation, please contact the Elections Division Help Desk

1-800-540-5954
(603) 271-8341
NHVotes@sos.nh.gov

Attorney General’s Office Election Line
1-866-868-3703
Elections@doj.nh.gov