Repeat clickers pose an increased risk as they have been proven susceptible to phishing simulations outside of the Organization’s risk tolerance.

91% of breaches start with an email.

50% more than half of cyber attacks are due to human error.

Potential Impact:
- Impact mail delivery system
- Damage physical and digital inventory
- Loss of sensitive personal information
- USPS reputational damage
While the Postal Service cannot prevent social engineering attacks to our network, we can reduce the risk of succumbing to these types of schemes.
Identifying suspicious emails is as easy as ABC(R)

A – Always look for the banner
B – Be on your guard
C – Careful of the hooks
R – Report
A - Always Look for the Banner

[EXTERNAL] Thank you for attending, review the presentation, download your viewing certificate...
• Once you’ve identified the email as [EXTERNAL], you should have a heightened sense of awareness and proceed with caution.

• Cyber criminals prey on human emotion and often have a sense of urgency.
C - Careful of the Hooks

1. Slow Down:
   Requests to take action “immediately” may indicate something is “phishy.”

2. Hover over Links:
   Use your cursor to hover over links. Here, it would have revealed a non usps.gov URL.

3. Ask Questions:
   Be skeptical. Would the Postal Service make this type of request?

From: Security Monitoring <SecurityMonitoring@liteblue-usps.com>
Sent: July 18, 2018
To: John A. Smith (Washington, DC) <john.a.smith@usps.gov>
Subject: [EXTERNAL] Urgent Security Event: Your account details were found online

Dear John Smith,

Security Monitoring Services recently found your account details online. To prevent unauthorized access of Postal systems using your information, take the following steps immediately:

1. Click <here> to review the information we have found
2. <Log in> to update your account credentials and password

Thank you.

Security Monitoring

Note: This message (including any attachments) contains confidential information intended for a specific individual and purpose.

4. Reach Out and Report:
   Contact the sender to verify. Here, you would find “Security Monitoring” does not exist in the Postal directory. Also, “liteblue-usps.com,” is not an official USPS domain, as indicated by the [EXTERNAL] label. If the sender seems suspicious, report to CyberSafe.

5. Keep Sensitive Information Private:
   Never share passwords or account credentials based on email requests.
[EXTERNAL] Thank you for attending, review the presentation, download your viewing certificate.

Report to CyberSafe
If you think you’ve been targeted

DO NOT…

- Forward the email
- Click any links
- Provide personal information (username or passwords)
- Open any attachment related to the message

Immediately report any suspected incident to the CSOC via the “Report to CyberSafe” button in Outlook, by calling 866-877-7247, or by emailing Cybersafe@usps.gov
From: Information Technology <IT@strongestpassword.com>
Subject: Password Check Required Immediately

Dear Staff,

As part of ongoing efforts to maintain regulatory compliance we have updated our password policy and we need everyone to check their password immediately to ensure that it meets our Minimum Security Requirements.

Please click here to do that:

Check Password

Please do this right away.

Thanks!
Information Technology
CAUTION: This email originated from outside USPS. STOP and CONSIDER before responding, clicking on links, or opening attachments.

All, We have made updates to the Delivering for America: Our Vision and Ten-Year Plan. Please click here to view the new document.

Louis
Below is the July phishing simulation email with annotated cues that should alert you of a phishing attempt. Don’t forget to use the SHARK approach when evaluating each message!

1. **S**low Down: Requests to take action “immediately” may indicate something is “fishy.”

2. **H**over over Links: Use your cursor to hover over links. Here, it would have revealed a non usps.gov URL.

3. **A**sk Questions: Be skeptical. Would the Postal Service make this type of request?

4. **R**each Out and Report: Contact the sender to verify. Here, you would find “Security Monitoring” does not exist in the Postal directory. Also, “liteblue-usps.com,” is not an official USPS domain, as indicated by the [EXTERNAL] label. If the sender seems suspicious, report to CyberSafe.

5. **K**eep Sensitive Information Private: Never share passwords or account credentials based on email requests.

---

From: Security Monitoring <SecurityMonitoring@liteblue-usps.com>
Sent: July 18, 2018
To: John A. Smith (Washington, DC) <john.a.smith@usps.gov>
Subject: [EXTERNAL] Urgent Security Event: Your account details were found online

Dear John Smith,

Security Monitoring Services recently found your account details online. To prevent unauthorized access of Postal systems using your information, take the following steps immediately:

1. Click <here> to review the information we have found
2. <Log in> to update your account credentials and password

Thank you.

Security Monitoring

Note: This message (including any attachments) contains confidential information intended for a specific individual and purpose.
Questions