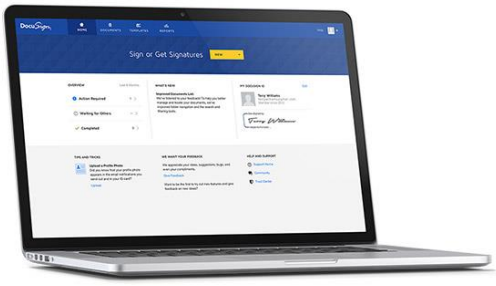
Monthly Cybersecurity Newsletter

March 2019 Issue

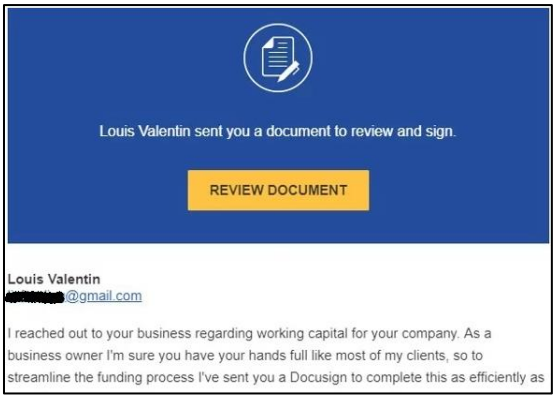
Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson



Docusign Scams: Not Your John Hancock!

There is a phishing scam that is not so new, but it could be making its way into your inbox soon. It will even pass the usual spam and malware filters and email protection devices. This is because this scam uses the DocuSign infrastructure with the standard DocuSign email notification. Since DocuSign is a well-known and trusted name, the vendor is a prime target for malicious phishing attacks that attempt to perpetrate fraud. If a person clicks on the standard yellow "Review Document" button in the DocuSign notification scam, he or she may receive a standard form requesting sensitive information that could be used to steal the person's identify or perpetrate other forms of fraud. If someone falls for this attack, the damage could be extensive, including financial loss and potential legal repercussions. Therefore, it is imperative for individuals to remain vigilant to this and other types of social engineering threats.



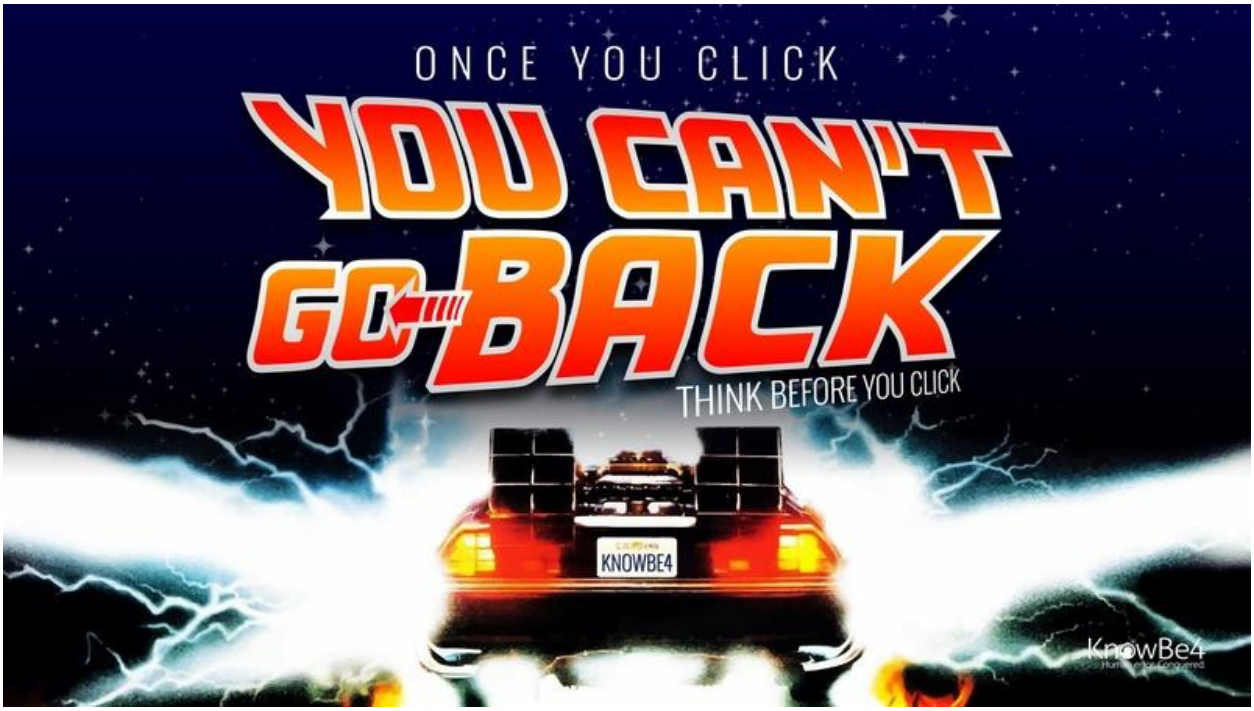
What Can You Do?

The following tips may help you avoid becoming a victim to a DocuSign phishing scam:

- Were you expecting the document, and do you recognize the sender? Contact the sender offline to verify the email's authenticity.
- Hover over the link – URLs to view or sign DocuSign documents contain "*docusign.net/*" and always start with "*https*".
- Access your documents directly from www.docusign.com by entering the unique security code, which is included at the bottom of every DocuSign email.
- Do NOT open unknown or suspicious attachments or click links. DocuSign will never ask you to open a PDF, an office document, or a zip file in an email message.
- Look for misspellings, poor grammar, generic greetings, and a *false sense of urgency*.
- Enable multi-factor authentication (MFA) where possible.
- Use strong, unique passwords and don't reuse passwords on multiple websites.

- Ensure your anti-virus software is up to date and all application patches are installed.
- Report suspicious DocuSign emails to report.spam@nc.gov and spam@docusign.com.

For more information, visit https://www.docusign.com/trust/security/incident-reporting.



>>>Monthly Newsletter

Don't forget the following resources available to you. The following are some other **cybersecurity newsletters** the ESRMO recommends. We hope you find them beneficial and share them with your peers!

Security Awareness Newsletter: A monthly security awareness newsletter that is provided by KnowBe4 for all State employees. ***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). The topic this month is ***How to Spot and Avoid Common Scams***.

- https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Disposing of Your Mobile Device.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link:

https://www.sans.org/webcasts/upcoming.

Cybersecurity Training and Awareness Plan

To combat the increasing security threats to the State's information systems and data, the Enterprise Security and Risk Management Office (ESRMO) will be providing, through the statewide Learning Management System (LMS), a series of cybersecurity awareness courses to be distributed every other month thoughout the 2019 calendar year. All Executive Branch employees and contractors are required to complete the assigned training modules by the end of each designated month. This training will be maintained in all employees' training records. The following is this year's Cyber Awareness Training Schedule:

Release Month	Lesson Topic	Lesson Title
March	Employee's Cyber Roles and Responsibility	Your role: Internet Security and You
May	Social Engineering	Phishing Fundamentals
July	Hardening Against Attacks	How to be a Human Firewall
**** JULY - ROLE BASED TRAINING [DBA & APPDEV] ****		
September	Information Protection	Understanding and Protecting PII
October	*****OCTOBER - CYBER AWARENESS MONTH*****	
November	Insider Threat	Insider Threat

This year, the ESRMO will also add **role-based training** for those who are Application Developers or Database Administrators. Agencies are required to identify those individuals with significant security responsibilities who operate in those two (2) positions. These individuals will be assigned an annual training module geared to their specific roles. The role-based training modules will be assigned by **July 1, 2019**, and must be completed within a 60-day period. The role-based training and the training for contractors who do not use the statewide LMS will be delivered through the training vendor portal, **KnowBe4**, from the following email address: ESRMO.Training@nc.gov. Contractors with state email accounts will receive an email with instructions on how to access their assigned training. Contractors are required to furnish the completion certificate to their supervisor for verification and retention.

KnowBe4
Human error. Conquered.

In addition to the scheduled training plan above, the ESRMO will also be conducting phishing exercises throughout the year via the preferred training vendor, **KnowBe4**. Phishing continues to be the *number 1 vector* used by malicious actors in order to gain access to systems and sensitive data. As part of our efforts to ensure employees do not fall victim to these attacks, the ESRMO will be conducting periodic unannounced phishing exercises on State government email accounts. Users who click on links in simulated phishing emails will be presented with additional training on ways to identify, detect and report these types of emails in the future. The goal of the phishing exercises, as well as the overall cybersecurity training program, is to raise awareness to users, decrease the possibility of compromise through phishing and other threats, and help better secure the North Carolina'sNorth Carolina's data and assets.

DO YOU RECOGNIZE THE SIGNS OF A SPEAR PHISHING EMAIL?

To: undisclosed-recipients is never a good sign.

From: Susan Molar <susanmolar@gmail.com>
Subject: UNITED NATIONS ORGANIZATION
Date: June 18, 2013 6:22:40 PM CDT
To: undisclosed-recipients;;
Reply-To: hansbruce@london.com

The From and Reply-To addresses are different.

Dear EMAIL OWNER/Fund Beneficiary,

We been authorized by United Nation secretary general, and governing body of the UNITED NATIONS Monetary Unit, to investigate the unnecessary delay on you payment, recommended and approved in your favor during the course of our investigation, we discovered that your Payment been Delayed by corrupt officials of the Bank who are Trying to divert you funds into their private accounts.

If you like receive you're funds thru this means you advised contact with Following information:

1. Your Full Name:

2. Address Where You Want the Courier to Send ATM Card

3. AGE

4. Occupation:

5. Telephone Numbers:

6. COUNTRY:

Requests for personal or sensitive information are usually scams.

NOTE: You are advised to furnish Mr. Hans Bruce with your correct and valid details. Also be informed that the amount to be paid to you is £1,000,000,00GBP. We expect your urgent response to this email to enable us monitor this payment effectively thereby making contact with MR.HANS BRUCE as directed to avoid further delay.

Congratulations.

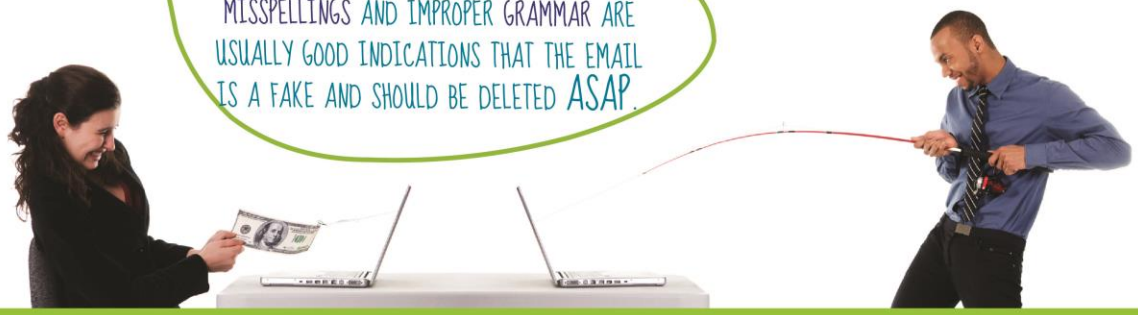
MR. KASSYM-JOMART TOKAYEV

DIRECTOR-GENERAL

UNITED NATIONS ORGANIZATION

Promises of money, threats or alarming messages, & deals too-good-to-be-true are common phishing email tactics.

Random capitalization, odd punctuation, misspellings and improper grammar are usually good indications that the email is a fake and should be deleted ASAP.



DON'T BE PHISHING BAIT.

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at **no cost** to government staff and contractors. With 60+ courses, all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated regularly.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ More than **60** available self-paced courses of varying proficiency – beginner to advanced
- ✓ Many popular certification courses including:
  - Network +
  - Security +
  - Certified Information Systems Professional (CISSP)
  - Windows Operating System Security
  - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework.
- ✓ Individuals can take courses to build their knowledge, skills, and abilities in cybersecurity.
- ✓ Taught by experienced cybersecurity subject matter experts.

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

"Hacking Humans" – A Podcast Covering Social Engineering!

Each week the CyberWire's **Hacking Humans** podcast looks behind the social engineering scams, phishing schemes, and criminal exploits that make headlines and take a heavy toll on organizations around the world. They talk to social engineering experts, security pros, cognitive scientists, and those practiced in the arts of deception. You will also hear from people targeted by social engineering attacks and learn from their experiences. To check out episodes of this podcast, visit the following page:

https://thecyberwire.com/podcasts/hacking-humans.html

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.