



# 2019 Boston

ANNUAL CONFERENCE  
& SHOWPLACE

## What HFAs and their Partners Need to Know about Cybersecurity: Breaches

Paul Cackler, Chief Information Officer

New York City Housing Development Corporation



# Types of Threats

- Ransomware
- Data Loss
- Business Email Compromise
  - Credential Phishing
  - Wire Fraud Scams
  - CEO Impersonation
  - Payroll Diversion



Jul 12, 2018

Alert Number  
**I-071218-PSA**

## **BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM**

This Public Service Announcement (PSA) is an update and companion to

September 10, 2019

Alert Number  
**I-091019-PSA**

## **BUSINESS EMAIL COMPROMISE THE \$26 BILLION SCAM**

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on [www.ic3.gov](http://www.ic3.gov). This

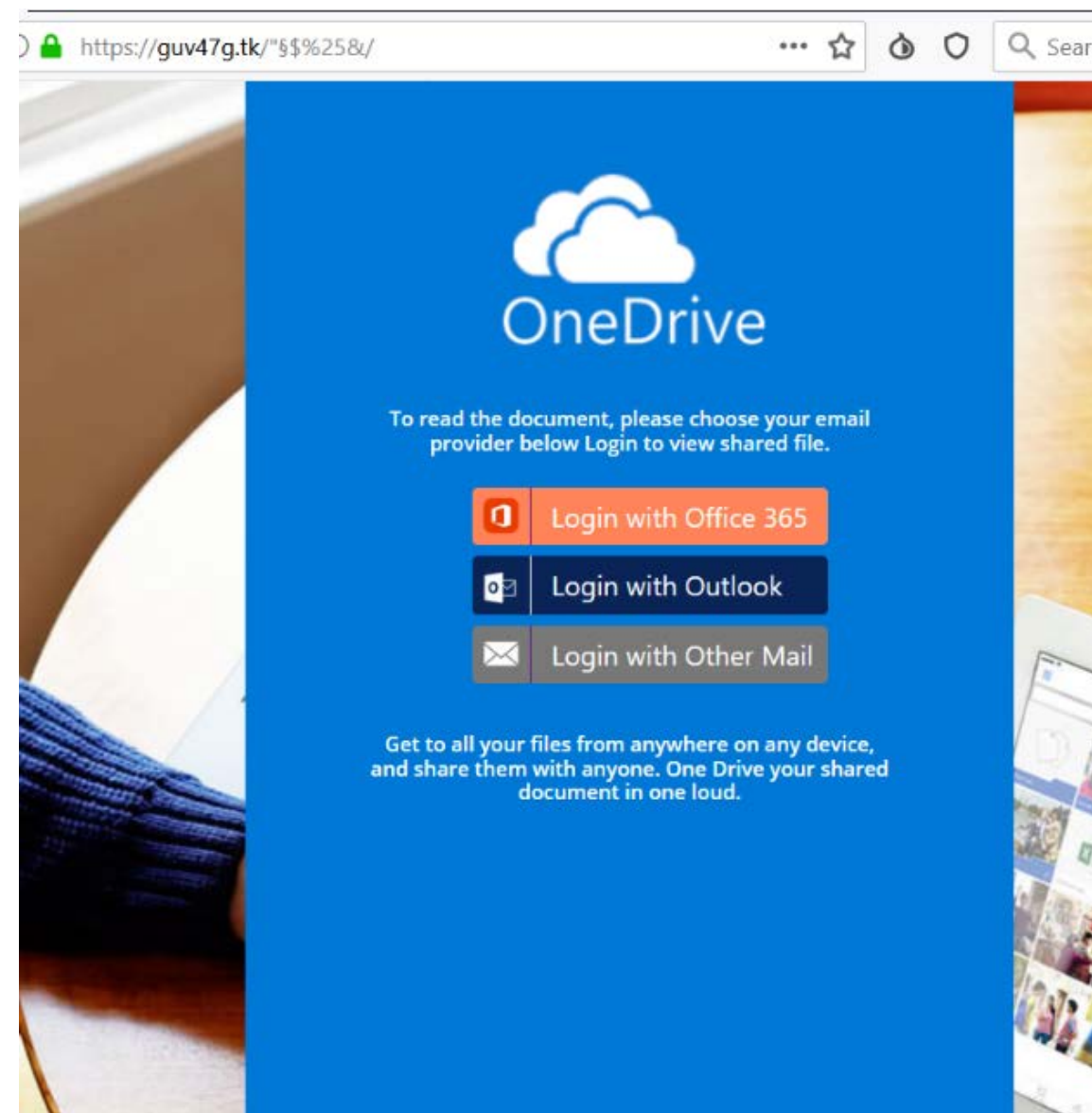
### **REAL ESTATE SECTOR TARGETS**

BEC/EAC actors heavily targeted the real estate sector in recent years.



# Credential Phishing

- Often an invitation to view a file
- The more sophisticated attempts come from a known contact whose email account has already been compromised
  - Someone you know
  - Someone you correspond with regularly
  - The email can come from their account
- Goal is to harvest your username and password






BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE S

EMOTET—

# World's most destructive botnet returns with stolen passwords and email in tow

Noticing an uptick in spam from people you know? You can probably blame Emotet.

DAN GOODIN - 9/19/2019, 2:45 PM

 SECURITY WARNING Some active content has been disabled. Click for more details. [Enable Content](#)

1. The first email account is compromised
2. A follow-up email is sent to the same thread, including conversation history
3. Includes a malicious Word document



## Accept the license agreement

You can use Microsoft Word until Friday, September 20, 2019. After that date, most features of Microsoft Word will be disabled.

To accept and start Word click Enable Editing and click Enable Content



# Wire Fraud Scams

- Web access to an email account obtained
- Mail rules are often setup
  - scan messages for certain keywords (wire, check, payment, etc)
  - forward email to another address
  - or, move email to an obscure folder and mark as read
- Take over the conversation and send new wire instructions
- The story creates a sense of urgency
  - “issue” with the previous bank account
  - need it today – will it be wired today – confirm receipt asap



## Symptoms of a Compromised Office 365 Email Account

Users might notice and report unusual activity in their Office 365 mailboxes. Here are some common symptoms:

- Suspicious activity, such as missing or deleted emails.
- Other users might receive emails from the compromised account without the corresponding email existing in the **Sent Items** folder of the sender.
- The presence of inbox rules that weren't created by the intended user or the administrator. These rules may automatically forward emails to unknown addresses or move them to the **Notes, Junk Email, or RSS Subscriptions** folders.
- The user's display name might be changed in the Global Address List.
- The user's mailbox is blocked from sending email.
- The Sent or Deleted Items folders in Microsoft Outlook or Outlook on the web (formerly known as Outlook Web App) contain common hacked-account messages, such as "I'm stuck in London, send money."
- Unusual profile changes, such as the name, the telephone number, or the postal code were updated.
- Unusual credential changes, such as multiple password changes are required.
- Mail forwarding was recently added.
- An unusual signature was recently added, such as a fake banking signature or a prescription drug signature.

# CEO Impersonation & Payroll Diversion

- Cybercriminals use social engineering to impersonate CEOs and high-level executives by spoofing the company email address
- Staff receive an email “from the CEO” requesting an invoice to be paid or their direct deposit to be changed to a new bank account
- May also request sensitive data such as employee W-2s, etc
- A recent case used a phone call with AI-generated audio (CEO voice “deepfake”)



CYBERSECURITY

## A new wire fraud scam targets your direct deposit info and sends your paycheck to a criminal's account

PUBLISHED TUE, APR 9 2019 3:52 PM EDT  
UPDATED WED, APR 10 2019 11:53 AM EDT



Kate Fazzini  
@KATEFAZZINI

# Important Security Measures

- Firewall, Intrusion Detection System, external port scanning, internal system vulnerability scanning and patching
- Virus scanning and malware detection (both on incoming email and on desktops and servers)
- User Training
- Multi-Factor Authentication and monitoring of log-in locations
- Identifying external emails and/or user impersonation flagging
- Aggressive web filtering and blocking
- Data Loss Prevention tools and email encryption