# Fraud Solutions in the Public Sector

Charley Wise, Public Sector Relationship Manager

Susie Todaro, Public Sector Payments

KeyBank
Use the red key.®

OHIO GFOA

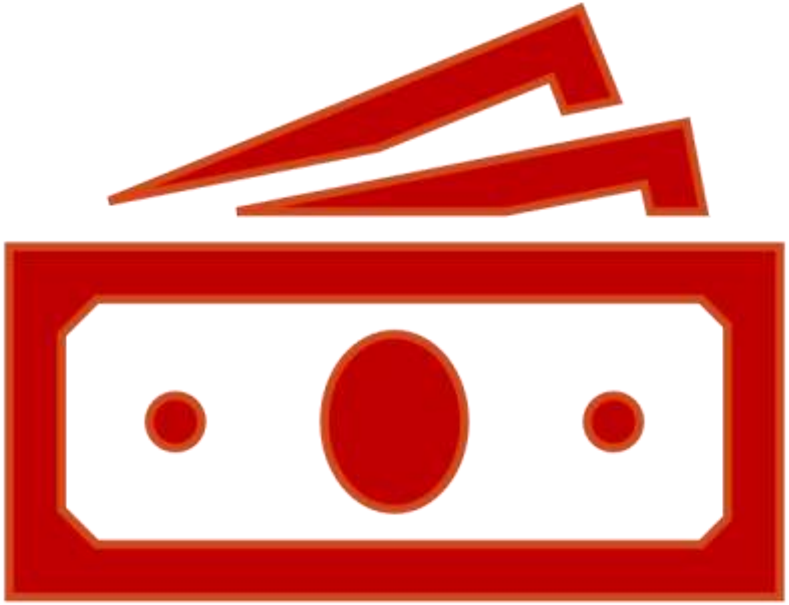
# Agenda

I. Cybersecurity / Types of Fraud

   A. Business Email Compromise
   B. Social Engineering
   C. Account Takeover
   D. Malware/Ransomware
   E. Vendor Payment Fraud
   F. Check Fraud
   G. ACH Fraud

II. Protect your accounts

   A. Password Security
   B. Payee Positive Pay
   C. ACH Blocks/Filters



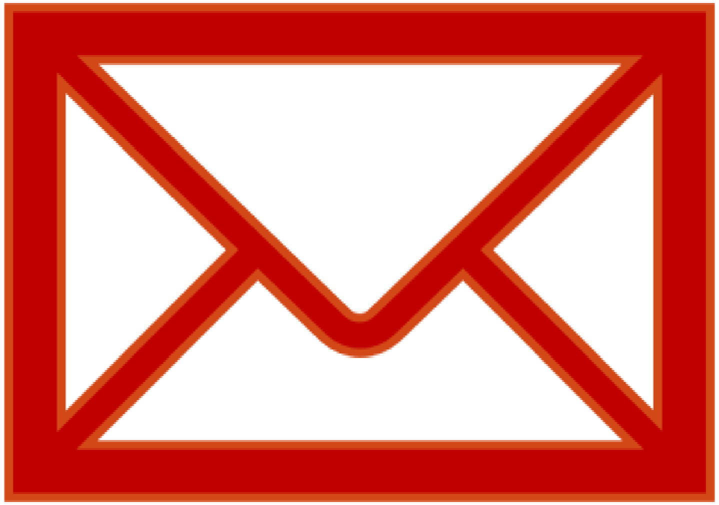
OHIO GFOA

# Introduction

One of the best ways to combat fraud is for you and your staff to become experts in the ways fraudsters try to gain access to your information and exploit your natural instincts to be helpful. By familiarizing yourself with the scenarios to follow, you will be able to recognize and stop scam attempts in their tracks.

# Business Email Compromise

Business email compromise (BEC) is a type of email cyber crime scam in which an attacker targets businesses to defraud the company. Business email compromise is a large and growing problem that targets organizations of all sizes across every industry around the world. BEC scams have exposed organizations to billions of dollars in potential losses.



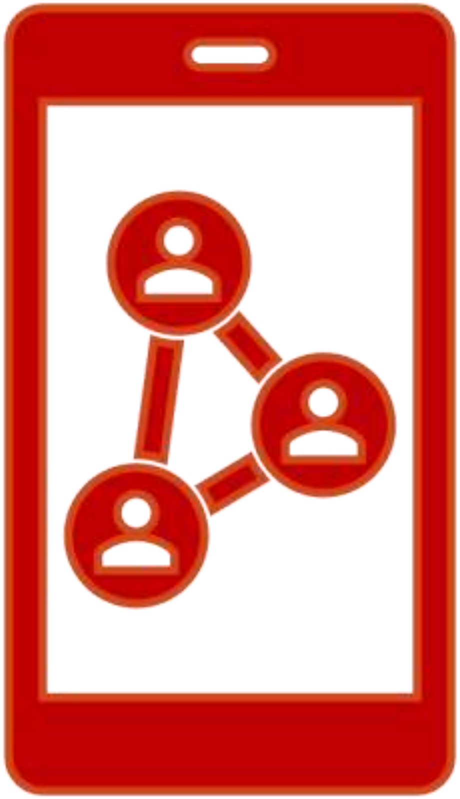
## Social Engineering

Includes phishing (email), vishing (voice call), or smishing (SMS/Text)

Fraudster misrepresents themselves as a legitimate business vendor, service provider, or other business partner in attempt to gain access to the client’s computer and/or obtain sensitive information

# Account Takeover: Mobile & Online Banking Fraud

Fraudster gains access to one or more online users' sign-on credentials and has attempted or been successful with sending funds to a fraudulent account



## Malware and Ransomware

- Malware:

Software unknowingly installed on the client’s computer specifically designed to harm and/or gain unauthorized access to data that can be used for financial gain

- Ransomware:

Client’s access to computer operating system is blocked by means of malicious software until fee is paid to attackers

Generally aimed at individuals, but becoming more prevalent with business entities

# Vendor Payment Fraud

Fraudster instructs insurance client or vendor to change the service provider’s settlement account

Unauthorized account change permits the fraudster to direct large dollar ACH transactions to the fraudulent settlement account

OHIO GFOA

# Protect Your Accounts

# Passwords Matter…a LOT!

- 90% of passwords are vulnerable to attack. *Avast*

- 40% of people have had their identities hacked, passwords compromised, or sensitive information breached because of duplicate and outdated passwords. *Web Tribunal 2023*

- Over 80% of data breaches are due to poor password security. *Indagent*

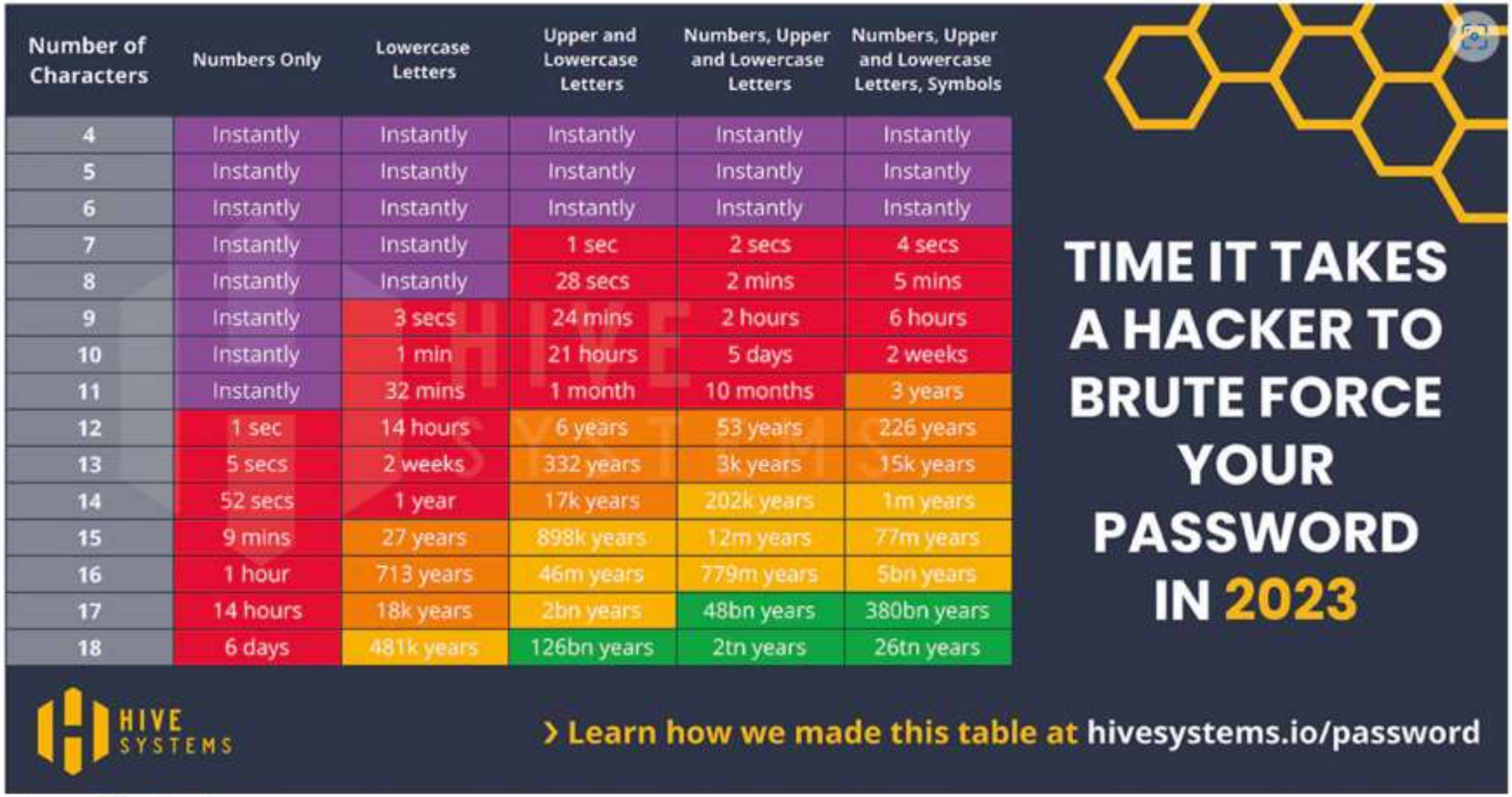
- 70% of breached passwords are still in use. *Spycloud*

- 64% of consumers repeat passwords across multiple accounts.

- In 2022, the fourth most common password was “password.” *Cybernews*

OHIO GFOA

# Password Security



| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 1 sec | 2 secs | 4 secs |
| 8 | Instantly | Instantly | 28 secs | 2 mins | 5 mins |
| 9 | Instantly | 3 secs | 24 mins | 2 hours | 6 hours |
| 10 | Instantly | 1 min | 21 hours | 5 days | 2 weeks |
| 11 | Instantly | 32 mins | 1 month | 10 months | 3 years |
| 12 | 1 sec | 14 hours | 6 years | 53 years | 226 years |
| 13 | 5 secs | 2 weeks | 332 years | 3k years | 15k years |
| 14 | 52 secs | 1 year | 17k years | 202k years | 1m years |
| 15 | 9 mins | 27 years | 898k years | 12m years | 77m years |
| 16 | 1 hour | 713 years | 46m years | 779m years | 5bn years |
| 17 | 14 hours | 18k years | 2bn years | 48bn years | 380bn years |
| 18 | 6 days | 481k years | 126bn years | 2tn years | 26tn years |

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Source: Hive Systems

# Secure Passwords, Simplified

Creating and maintaining strong passwords isn’t as difficult as you might think.

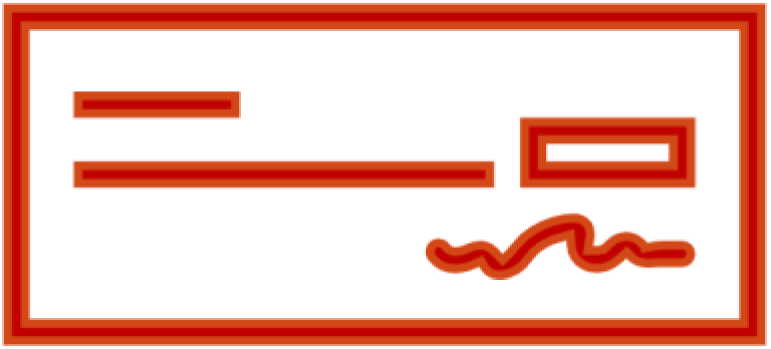
- ***Think passphrases, not passwords*** – A passphrase is a sequence of words or a sentence that is easy to remember but difficult to guess – and is much more secure than a single word. "MyDogIsTheBest#1" is a stronger password than "buddy123."

- ***Enable two-step verification, when offered*** – Two-step verification adds an extra layer of security by requiring a code or token in addition to your password to access an account. This makes it more difficult for a hacker to gain access even if they have your password. In fact, multi-factor authentication blocks 99% of all password safety issues, according to Microsoft.

- ***Use a password manager software*** – A password manager is a tool that generates and stores secure passwords for you. It can help you manage and organize all of your passwords in one place.

OHIO GFOA

# Check Fraud



OHIO GFOA

# Check Fraud

- Check fraud is not a new phenomenon. But recently, new techniques like check washing, organized criminal rings, and post office vulnerabilities have driven a major increase in reports of check fraud. The Financial Crimes Enforcement Network (FinCEN), a division of the U.S. Treasury Department, issued an alert in February of 2023, warning financial institutions of a "**nationwide surge in check fraud schemes targeting the U.S. Mail.**"

- According to FinCEN, financial institutions filed more than 350,000 reports of potential check fraud in 2021—a 23% increase from 2020. In 2022, the number of filings **nearly doubled to 680,000**. And these days, fraud of all kinds is big business: the FBI's Internet Crime Complaint Center (IC3) reports that between 2018 and 2022, it received 3.26 million complaints, reporting a loss of $27.6 billion.

- Recent research from the Association of Financial Professionals indicates that checks continue to be the payment method impacted most often by fraud activity. 63% of financial professionals surveyed reported that their organizations faced some kind of check fraud activity in 2022. And while businesses use fewer paper checks than they used to, 71% of survey respondents said that their organizations are using checks, and three-quarters of organizations that currently use checks do not plan to discontinue their use.

- One driver of increased check fraud was the relief payments issued periodically throughout the COVID-19 pandemic. The government mailed thousands of physical checks to U.S. citizens, which increased opportunities for criminals to steal checks from the mail and use them to commit check fraud.

# Check Fraud - Prevention

- **Reduce check use**. The best way to prevent check fraud is to reduce or eliminate payments by paper check. In addition to helping businesses avoid fraud, digital payment platforms can help lower the cost of paying vendors and suppliers.

- **Use available tools that catch fraud**. Banks offer a range of tools to mitigate the risk of check fraud. For example, Key's Positive Pay service provides fraud detection reporting by comparing items presented for payment against the check details provided in your issuance file. Any checks that do not match are presented to you for review and payment disposition (pay/no-pay decisions). These tools are already widely in use by large businesses that issue thousands of payments every week. But with check fraud on the rise, businesses of all shapes and sizes need to strengthen their internal controls.

- **Daily reconciliation**. Last but not least, if you must issue paper checks, make sure to reconcile your business accounts every day and immediately report any suspicious or obviously fraudulent activity to your bank. Additionally, businesses should implement a tightly controlled check-printing process, and limit employee access to check stock. Finally, with check theft via the USPS on the rise, avoid sending checks through the mail unless absolutely necessary.

# ACH Fraud

# ACH Fraud

- **Payment Authorization / Blocks / Filters** - combat fraud by automatically comparing incoming ACH credit/debit attempts to your electronic authorization files. You are notified of any items that are not pre-approved, and then you notify the bank if you would like to pay or return the items.

- **Universal Payments Identification Code (UPIC)** - secure bank account identifiers that allow you to receive electronic payments without exposing account information that can leave you vulnerable to fraud.

- **Account Validation** – perform due diligence and ensure the legitimacy of customer/vendor accounts prior to making or receiving payments.

# Questions / Answers

# Thank you!!