

The background features abstract, overlapping geometric shapes in various shades of green, ranging from light lime to dark forest green. These shapes are primarily located on the left and right sides of the frame, creating a modern, layered effect. The central area is a plain white space where the text is located.

Don't become  
a fraud statistic

# The Fraudsters Want You!

- ▶ Business Email Compromise
- ▶ Payroll Diversion
- ▶ Payment Redirect Fraud
- ▶ Ransomware
- ▶ Extortion tied to Data Breach



# Business Email Compromise

- ▶ Spear Phishing Attempt
- ▶ Targets financial and payroll professionals
- ▶ Undetectable by anti-virus and spam filters
- ▶ Well researched and well written
- ▶ Highly Successful
  - ▶ 48% of targets reported taking a loss

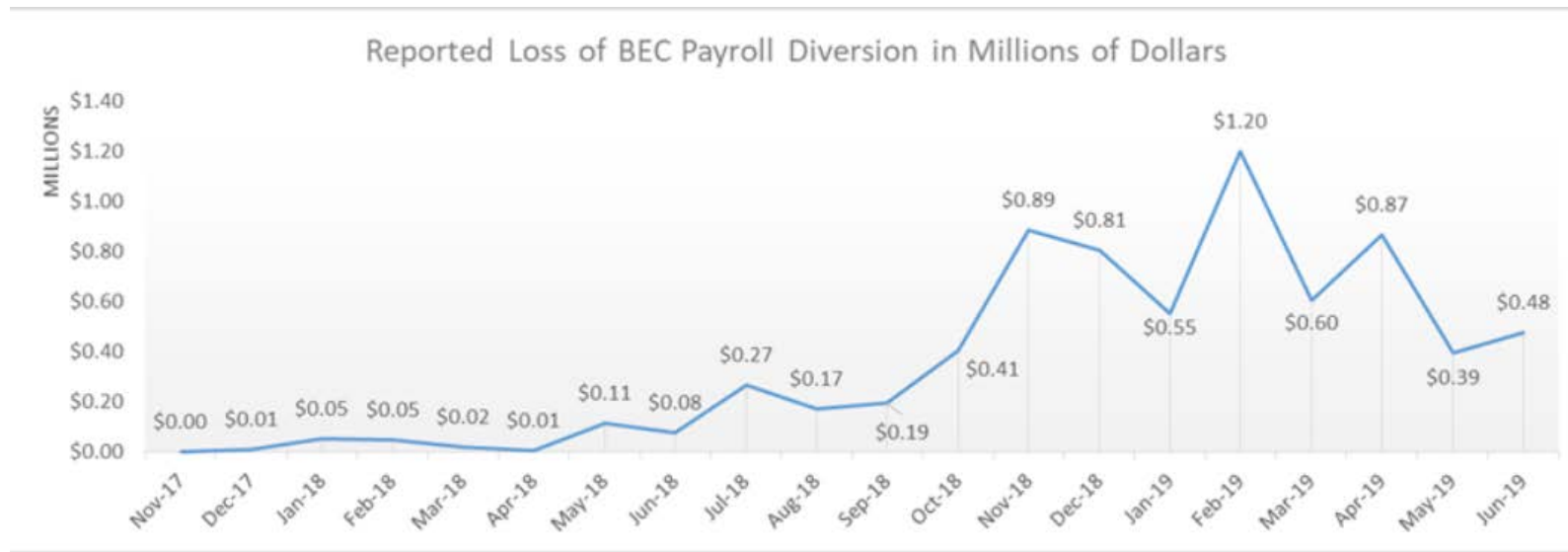
# The Request to Transfer Money

- ▶ Email from an Executive
  - ▶ Address Spoofed
- ▶ Creates a sense of urgency
  - ▶ Urgent, Immediately, Important, Emergency, Disgruntled Citizen/Client, Now
- ▶ Keep Secret
  - ▶ Don't tell anyone, You're the only one I can trust, I'm counting on you
- ▶ Unavailable
  - ▶ Out of office/town, In meetings, Working from home, Extremely Busy

# Payroll Diversion

- ▶ A form of Business Email Compromise
- ▶ Email purporting to be from employee
- ▶ Social engineering to obtain employee credentials
- ▶ Requests account change or copy of W-2/W-4
  - ▶ Payroll is diverted to fraudster's account
  - ▶ Info on tax forms used to compromise employee accounts

# Payroll Diversion Losses



Source: Internet Crime Complaint Center (IC3)

# Payroll Update Best Practices

- ▶ Require completed state forms
- ▶ Independent verification: in person/telephone
- ▶ Provide employee written confirmation of account changes

# Payment Redirect Fraud

- ▶ Request to update Vendor's banking details
- ▶ Account contact information changes w/o introduction
- ▶ Instructions not to contact HQ
- ▶ Invoice Anomalies: Format change, letterhead/logo changes



# Transparency = Vulnerability

- ▶ Open Check Book
- ▶ Public Record Requests
- ▶ Statewide Vendor Number Look-up
- ▶ Forms available online

# Ransomware

- ▶ Malware that encrypts victim's computer or servers
- ▶ Fraudsters favor governments, law enforcement, health care providers and critical services
- ▶ FBI discourages payment
  - ▶ Victims may not receive decryption key
- ▶ Recovery usually expensive

# Grays Harbor Community Hospital

- ▶ Occurred in July reported in August
- ▶ Successful Phishing attempt likely cause
- ▶ Medical Record databases encrypted
- ▶ Unable to process payments
- ▶ \$1 million worth of Bitcoin demanded
- ▶ Recovery costs remain unreported
- ▶ <https://www.ghcares.org/news/releases/grays-harbor-community-hospital-provides-notice-of-recent-ransomware-attack/>
- ▶ <https://www.thedailyworld.com/news/records-of-85000-involved-in-hospital-hack/>

# Protect Yourself

- ▶ Be suspicious
  - ▶ Emails from unknown senders
  - ▶ It's urgent or 'the sky is falling'
  - ▶ Coupon or something for nothing offers
- ▶ Watch for spoofed email addresses
- ▶ When in doubt call... do not call number provided in email
- ▶ Don't open attachments or links unless you know the sender
- ▶ Never provide personal information or login credentials

# KNOWBE4 – Phishing Subject Lines




## Top Ten Successful Phishing Test Attacks

- ▶ Password Check Required Immediately
- ▶ De-activation of (email) in Process
- ▶ Urgent press release to all employees
- ▶ You have a new voicemail
- ▶ Back up your Emails
- ▶ Revised Vacation & Sick Leave Policy
- ▶ UPS Label Delivery, 1ZBE312TNY00015011
- ▶ Please Read Important from Human Resources
- ▶ (manager name) sent you a file on Box
- ▶ Important message from (company name) Admin

## Top Ten Reported Successful “In the wild” Attacks

- ▶ eBay: Important your account
- ▶ Google: Your photo has been successfully published
- ▶ Outlook/Microsoft: You’re invited to share this calendar
- ▶ Secure your Btc wallet now
- ▶ Amazon: Account refund verification status
- ▶ Unusual sign-in activity
- ▶ Check sent
- ▶ LinkedIn: LinkedIn password reset
- ▶ Warning: Unauthorized software detection
- ▶ Microsoft: You’ve been assigned a task!

# Phishing Attempt

 Reply  Reply All  Forward



Fri 10/11/2019 9:15 AM

Duane A. Davidson <offislist@earthlink.net>

**Re: Urgent**

To Williams, Lesa (TRE)

Was wondering if you've had a chance to quick errand... Do let me know if....!!!!

- ▶ Sent to several OST employees
- ▶ Included an attachment (stripped by anti-virus)
- ▶ Note the email address

# Extortion Tied to Data Breach

- ▶ Extortion by email or snail mail
- ▶ Includes personal information obtained through data breach
- ▶ Threat to expose 'compromising info'
- ▶ Demands 'untraceable' payment
  - ▶ Cryptocurrency
  - ▶ Gift Cards

# Resources

- ▶ Internet Crime Complaint Center (IC3)
  - ▶ <https://www.ic3.gov/crimeschemes.aspx>
- ▶ FBI Scams and Safety
  - ▶ <https://www.fbi.gov/scams-and-safety/common-fraud-schemes>
- ▶ Krebs on Security
  - ▶ <https://krebsonsecurity.com/>