Recognizing Cyberfraud

Learning to recognize fraud tactics

October 2023

"Most people think criminals break into their computers and devices. In most instances, you're the one who is giving access to the crooks."

Burton Kelso

The Technology Expert

burtonkelso.com

Fraud is big business.

Source: AFP 2023 Payments Fraud and Control Survey Report

Taking Advantage of Human Nature

- Some schemes directly steal money, while others go after employee credentials (usernames, passwords, etc.) and sensitive company data.
- Today's cybercrime is designed to take advantage of key elements of human nature—trust and the desire to please superiors—as well as the pressure business people feel to complete tasks quickly.
- All people-focused attacks have one thing in common—they rely on identity deception.

Source: AFP 2022 Payments Fraud and Control Survey Report

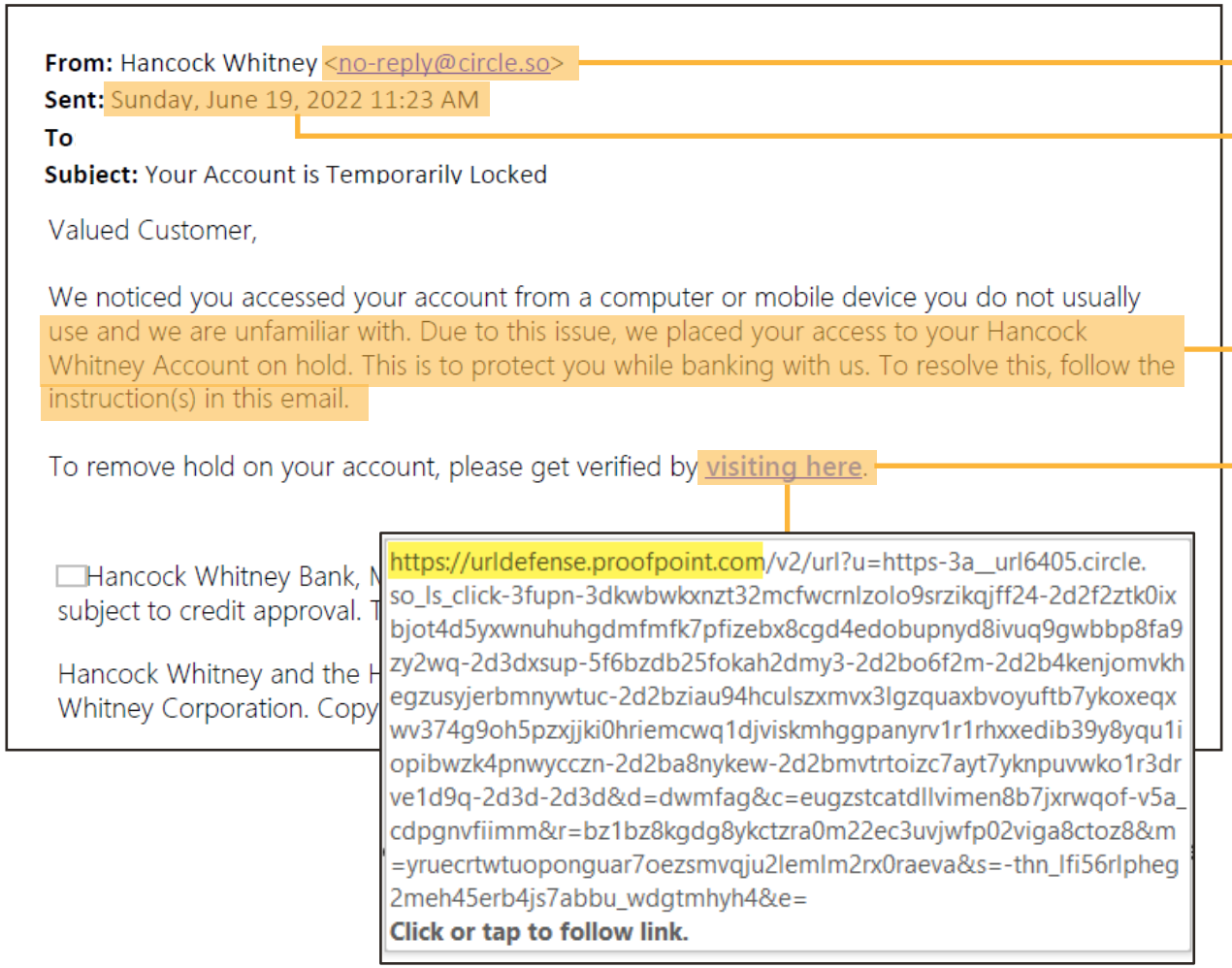
Types of Fraud

Business Email Compromise (BEC) Scams

- **BEC** — In a typical attack, a key employee (often in the accounting department) is targeted for an email that attempts to trick the employee into sending money to the crook.
- Spoof email or website: sends victims a forged email to trick users into thinking the email or website is legitimate.
- Domain look-alike: Fraudsters create look-alike domains to confuse victims into believing they are on a legitimate site. These sites lead to web traffic diversion and malware.
- Legitimate email that was taken over by a fraudster and sends victims "change of payment" instructions for an invoice or payroll diversion.

Source: AFP 2023 Payments Fraud and Control Survey Report

How to Spot BEC Scam



The email address is incorrect

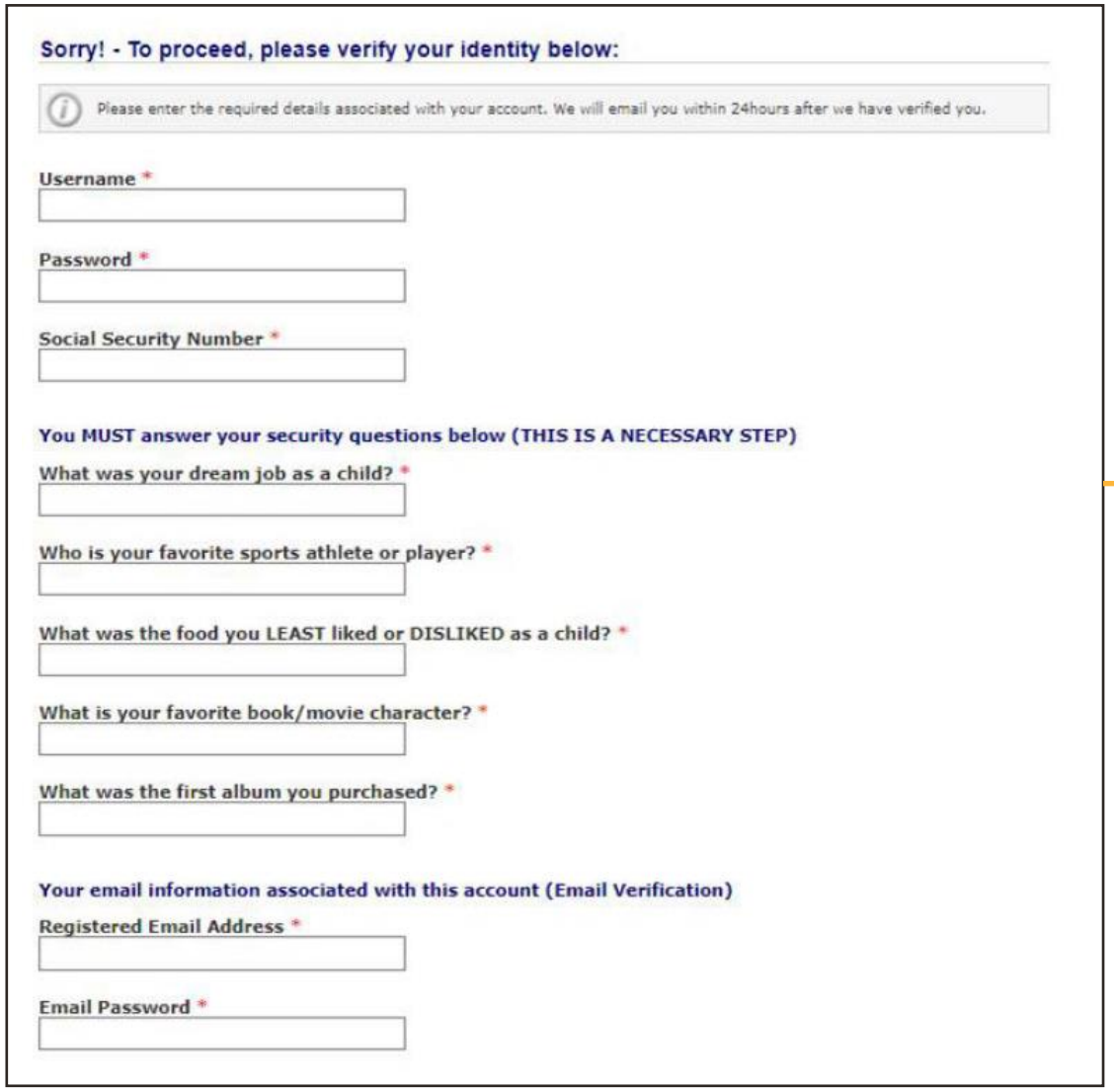
Date Sent

Expresses a sense of urgency

Scroll over hyperlink to see where it is taking you

HANCOCK WHITNEY

Spotting a Scam Form



If the hyperlink takes you to a page like this, it is a scam.

HANCOCK WHITNEY

ACH and Wire Fraud

How to Spot a Fraud Attempt

- The sender places a rush request:
  - Scammer insists the transfer take place immediately. Resist the hustle.
- The sender insists on communicating via email only:
  - If you can't verify the request, wait.
- The requestor—the CEO or executive—is out of the office:
  - Always verify this request with another executive before sending any funds.
- The nature of the request or the amount is unusual or inconsistent with prior experience:
  - If it is out of the ordinary, definitely be suspicious.
- The email address or other details in the request are wrong:
  - If it looks strange, don't fulfill the request without getting authorization.

Source: AFP 2022 Payments Fraud and Control Survey Report

Steps to Take Before You Pay

- Verify by two forms of communication (for example, known phone number and known email address) before you send funds.
- Be cautious of new payment information.
- Match your payment to a legitimate invoice before paying.
- Verify before clicking on a link or opening an attachment in an email or text.
- Double-check the email address.
- Do not respond to email as verification.
- Beware of a sense of urgency.

Check Fraud

- Check fraud can be done either by altering checks or counterfeiting checks.
- A scammer can alter information on a stolen check, such as the recipient's name and amount, then deposit a higher-dollar version of the item into their own account. Or the criminals have your stolen check information to create counterfeit copies. Today's technology makes printing a slew of look-alike counterfeit checks easier than ever.
- 63% of all businesses that experienced fraud in 2022 were victims of check fraud.

Source: AFP 2022 Payments Fraud and Control Survey Report

To Combat Check Fraud, Review Your Internal Process

- Reconcile bank accounts daily in order to check for any irregularities.
- Make sure that the authorized signers of company checks are not the same people who reconcile the account.
- Review all hiring procedures—know your employees.
- Make sure two people are responsible for accounts payable.
- Make sure that mailroom personnel and procedures are sound.
- Keep all check stock or cash equivalents in a secure and locked facility.
- Change keys or entry codes periodically to prevent routine access to storage areas.
- Consider surprise audits.
- Consider moving check disbursement activity to electronic payment.
- Use Positive Pay for check and ACH payments.

Spear Phishing

- **Spear phishing** — emails designed to trick targeted individuals into performing a task for the thief (like sending a wire or ACH payment to an account controlled by the fraudster)
- Why do spear phishing attacks succeed?
  - **Simplicity** — The request seems normal. The crook asks victims to perform tasks that fall under their normal duties. The request looks authentic; it contains wire details and an amount.
  - **Today's corporate culture** — Employees are available 24/7; they respond quickly to solve a problem.

Source: AFP 2022 Payments Fraud and Control Survey Report

More Fraud Tactics

- **Social engineering** — online schemes that use deception to manipulate victims into divulging sensitive information, login credentials or data
- **Malware** — malicious software designed to disrupt, damage or gain unauthorized access to a computer system for nefarious purposes

Bottom Line

- Check accounts daily for suspicious transactions.
- Don’t click on hyperlinks or attachments from unknown sources.
- Be aware of “too good to be true” offers.
- Verify, verify, verify. If it involves sending money, make sure you know who the money is going to.
- Review your fraud processes and procedures annually with your banking partners.

Key Takeaways to Remember

The first line of defense in fraud prevention is you.

Change your focus from “ASAP” to “As Securely As Possible.”

For more information visit Hancock Whitney Cybersecurity For Business

hancockwhitney.com/cybersecurity-for-business