

Protecting
Your County's
Financial
Assets in a
Changed
Environment



**AMERIS
BANK**

Kevin Strickland
Director of Nonprofit and Association Banking
Kevin.Strickland@amerisbank.com
850-661-3972



Florida's Recent Cyber Attacks

- **2019:** Collier County scammed out of \$184K as a result of a business email compromise.
- **2019:** The City of Tallahassee had \$500,000 redirected out of the employee payroll account.
- **2019:** The City of Riviera Beach paid \$600,000, after hackers ransomed the city's encrypted data.
- **2020:** The City of Naples lost \$700,000 as a result of a cyber attack by an imposter representative from a construction firm contracted by the city.
- **2021:** A hacker tried to increase the levels of sodium hydroxide by gaining access into the water treatment system of Oldsmar, Florida

The New York Times

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers \$600,000

THE WALL STREET JOURNAL.

Hackers Strike Another Small Florida City, Demanding Hefty Ransom

Lake City officials agree to pay \$462,000; 'There are a lot of copycats out there'

Almost \$500,000 swiped in city of Tallahassee payroll hack

Karl Etters Tallahassee Democrat

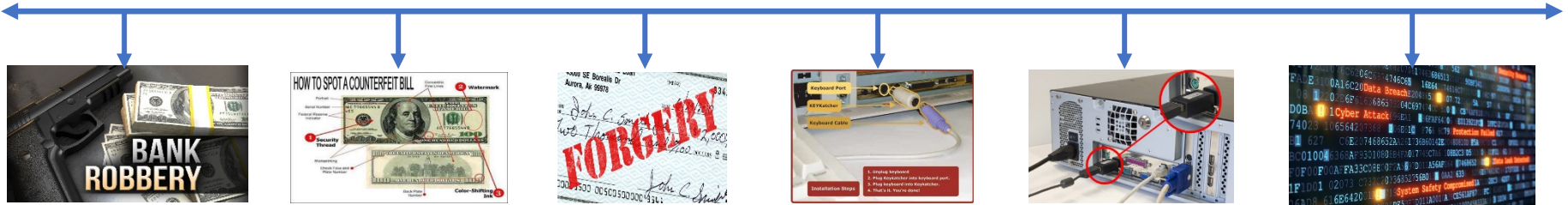
Riviera Beach pays massive ransom to hackers following cyber attack, official says

Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says

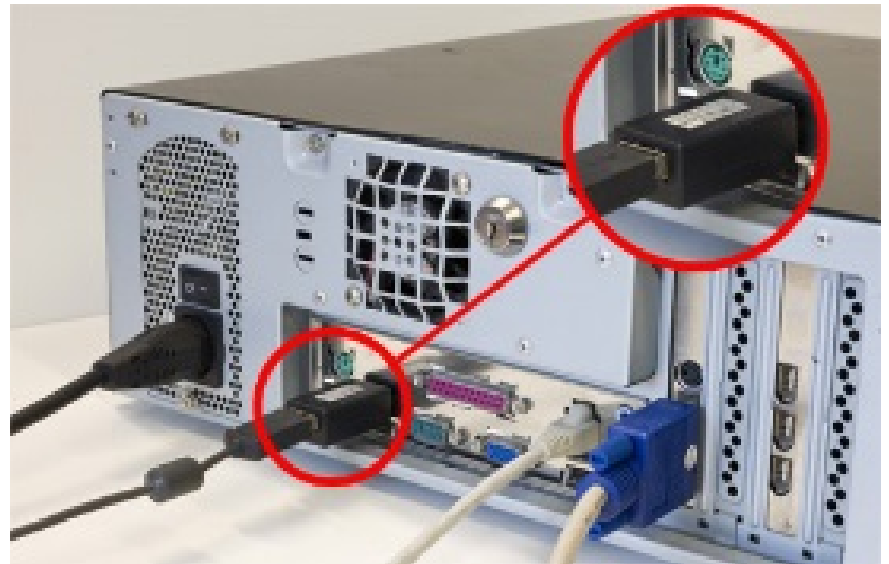
By Amir Vera, Jamiel Lynch and Christina Carrega, CNN



The Evolution of Fraud



- Bank robbery
- Counterfeit currency
- Forged, counterfeit checks
- Keyloggers
- Digital age



Today's Topics

WHITE-WASHED CHECKS

Mail snatchers erase the ink on a **check** with chemicals found in common household cleaning products.

BUSINESS EMAIL COMPROMISE

Form of cyber crime which use email fraud to attack commercial, government and non-profit organizations.

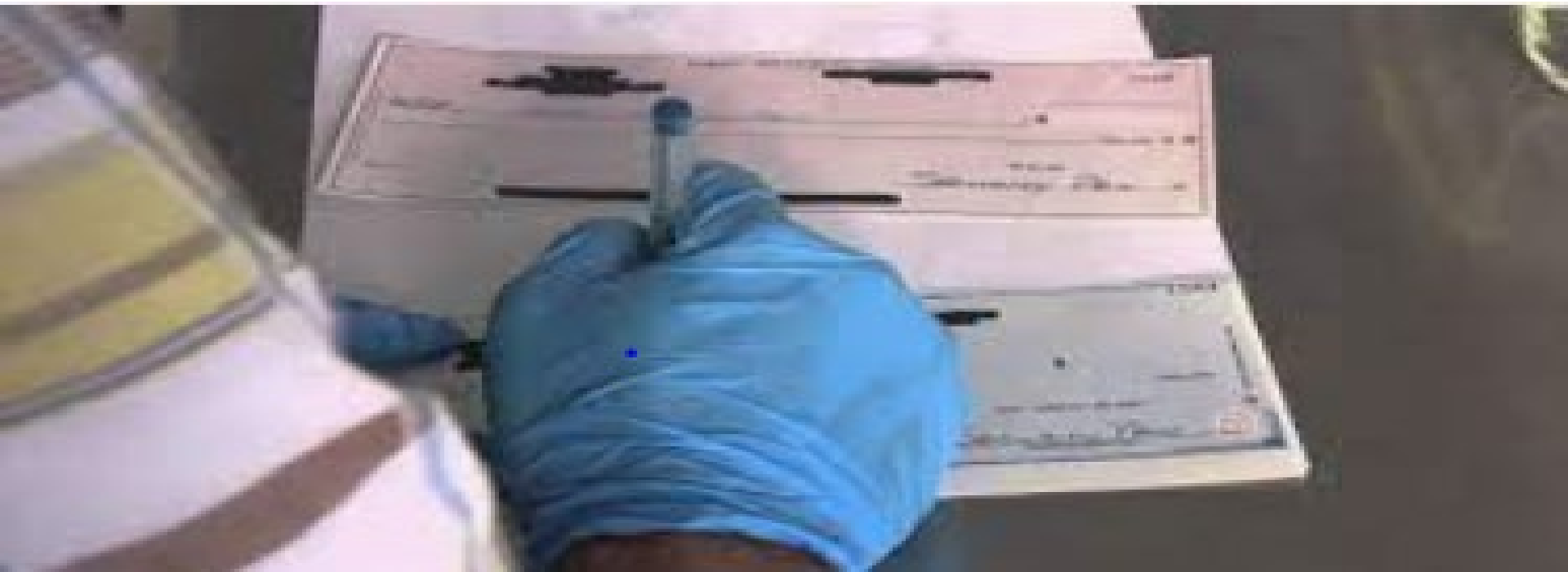
INTERNAL FRAUD/EMBEZZLEMENT

The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.

RANSOM WARE

Threatens to publish your organization's data or perpetually block access to it unless a ransom is paid.





Scheme #1: White-Washed Checks



White-Washed Checks Statistics

- The FBI estimates that losses from check fraud total **\$18.7 billion annually**.
- More than **500 million checks**, more than a million a day, are forged annually in the U.S.
- The average fraud scheme lasts **18 months** before it is detected.
- The most common method for detecting fraud is through **tips from employees, customers, vendors** and anonymous sources.
- The second most common method of discovery is by ***accident***.



White-Washed Checks

- Mail snatchers erase the ink on a check with chemicals found in common household cleaning products found on the shelves of your local Walmart (Bleach, carpet cleaner, carbon tetrachloride or nail polish)
- Check are re-written, increasing the amount payable by hundreds and even thousands of dollars.





Scheme #2

Business Email Compromise:

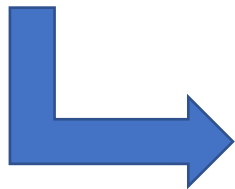
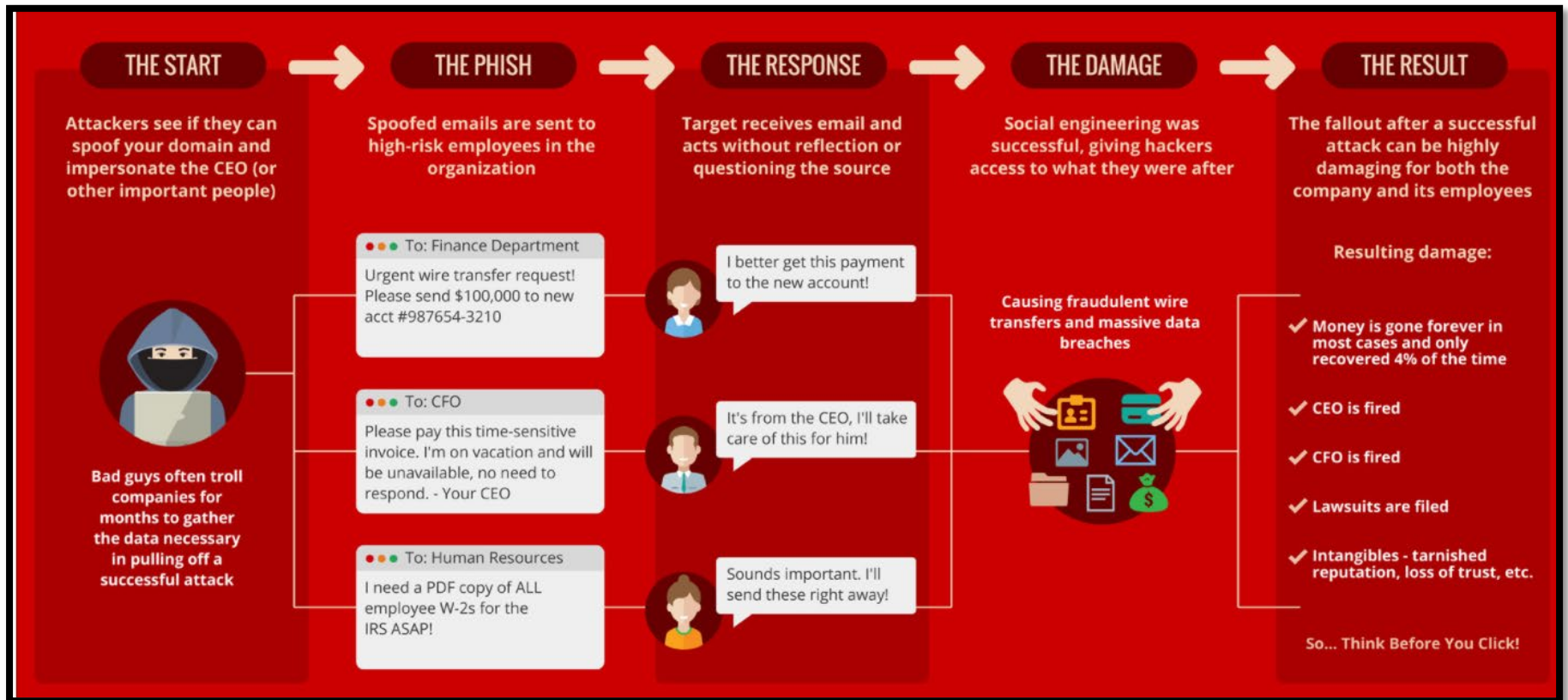


Business Email Compromise (BEC) Statistics

- Between May 2020 and July 2021, there was a 100 percent increase in identified global Business Email Compromise exposed losses (Internet crime complaint center)
- Over the past three years, Business Email Compromise (BEC) schemes have caused at least \$5.3 billion in total losses to approximately 24,000 companies around the world (trendmicro)
- During the third quarter of 2020, the median number of business email compromises received per company each week rose by 15% (techrepublic)
- 65% of companies faced business email compromises in 2020 (security Blvd.)



Business Email Compromise: Spear Phishing



Look at the spelling of the words and names carefully.

Tom.rogers@mycomp.com

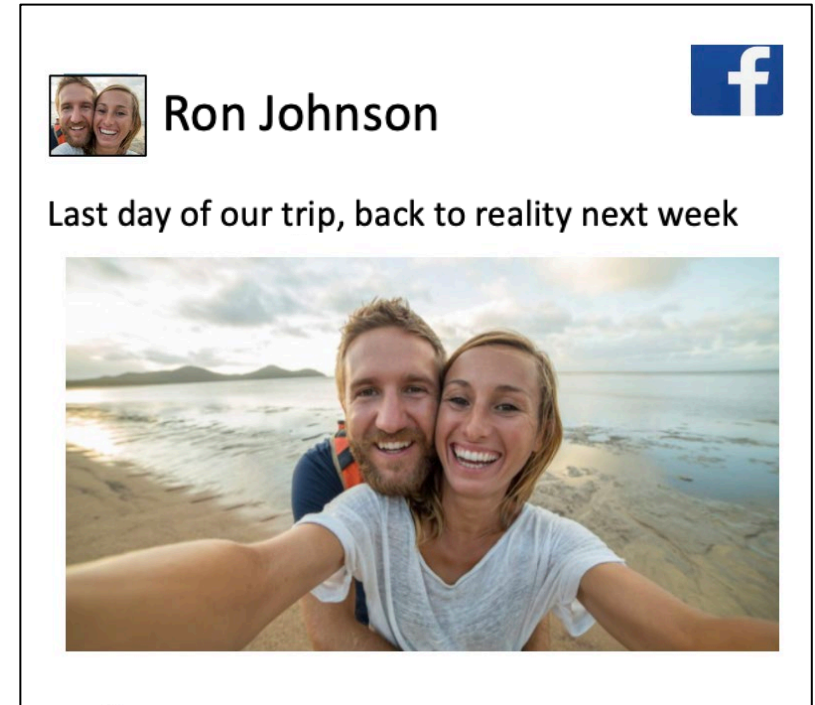
Tom.rogers@rnycomp.com

www.mircosoft.com



Business Email Compromise: Spear Phishing

- Perpetrators research key individuals and their roles in the company based on information on social media sites, professional associations, company website, etc.
- Crooks look at post for specifics such as job duties/descriptions, hierarchal information and out-of-town travel details
- Fake social media accounts can be created, appearing they are legitimate
- Information about the individual can be used to personalize and legitimize business email attacks.



Fraudsters often review social media sites to legitimize attempted email compromises



Business Email Compromise

The screenshot shows an Outlook interface with the following elements:

- Header:** Office 365 | Outlook
- Search Bar:** Search Mail and People
- Navigation:** New, Delete, Archive, Junk, Sweep, Move to, Categories, Undo
- Left Sidebar:** Folders, Groups (New), Browse groups, Create group
- Inbox:** List of emails including one from Katie Jordan titled "Summary of today's team meeting" (Sun 9:22 PM).
- Email Thread:**
 - From:** Katie Jordan (profile picture)
 - To:** Tom
 - Subject:** Summary of today's team meeting
 - Date:** Sun 8/30/2015 9:22 PM
 - Body:**

I'm in meetings and will be out of reach for the next couple of hours. I just negotiated a contract with a new vendor, Everlast Gen, Inc. to supply back up power to the district's pumps. Please instruct our bank to send a wire transfer from our reserve account to Everlast Generator Company in the amount of \$75,000. Everlast's routing number is 065494854 and their account number #123456. Please make sure you send the funds ASAP so we can secure our pricing. Please keep the news about the contract confidential until I announce it to the board tomorrow.

Invoiced Attached

P.S. Looks like you and Susan had a great time at at the beach last weekend, tell her I said hello.

Katie Jordan
General Manager, Crooksville Florida
 - Attachments:** Electroplex_Invoice_70006.pdf

Annotations:

- Hacked/Altered Email:** Points to the email header area.
- Sense of urgency:** Points to the highlighted text about the wire transfer.
- Personalized:** Points to the P.S. note about the beach.
- Bogus Invoice:** Points to the attached PDF file.

Sophisticated Cyber Criminals Do Their Homework



The Bogus Invoice

- Fraudster emails/mails an invoice to the company; often address to the AP department
- Invoice usually includes remittance information including the account to which funds are to be paid
- Invoice may include a link to pay the invoice online, the link may be a source of malware

INTERNET NETWORKX
PO BOX 957269
DULUTH, GA 30095-7269

Please make checks payable to: "Internet Networkx"

LISTING	DOMAIN/WEBSITE	AMOUNT
Annual Renewal IN-465400		\$194.00

Please Remit Payment by 5/22/2019






X01VJ8595983 DF0E44834

Annual Renewal

Date: 4/22/2019
Website: 
Number: 
Return By: 5/22/2019

WEBSITE: 

DESCRIPTION OF SERVICES:
ANNUAL RENEWAL WEBSITE LISTINGS
SERVICE FROM 5/22/2019 thru 5/22/2020 \$194.00

TOTAL FOR DNS LISTING RENEWAL: \$194.00

SUBSCRIPTION INCLUDE:
Annual Website Listings on internet directory for details visit—www.internetnetworkx.net
Please note: *name change from Web Domain Listing. Please email to update w9 on file.*
THIS IS NOT A BILL. THIS IS A SOLICITATION. YOU ARE UNDER NO OBLIGATION TO RENEW.

Thank you for your payment
We Appreciate Your Business!

INQUIRES: www.internetnetworkx.net CUSTOMER SERVICE: contactus@internetnetworkx.net
Please detach and return lower portion with your payment to ensure proper credit. Retain upper portion for your records.

Please return this portion with your payment

Return by 5/22/2019
IN-465400

Total due for annual renewal \$194.00

Please Make Checks Payable to "Internet Networkx"
To Pay with Credit Card, Use Authorization form below

petersonmetz.com

MAIL PAYMENT TO:
INTERNET NETWORKX
PO BOX 957149
DULUTH, GA 30095-7149



VISA_DISCOVER_MASTERCARD_AMEX
CARD# [REDACTED]
NAME ON CARD [REDACTED]
EXP. DATE / CVV AMOUNT \$ 194
ZIP [REDACTED] Text Receipt [REDACTED]
SIGNATURE [REDACTED]

☐ Note address changes on back

A Real-Life Example: Spear Phishing

1. A fraudster, posing as the CEO, sent an email to the legitimate CFO instructing them to wire a large sum of money to a outside contractor. The first email used below is fraudulent, the second is legitimate:
 1. Bob.Thompson_XYZ.FL.com
 2. Bob.Thompson-XYZ.FL.com
2. The CFO had been on vacation the week before, and it was their first day back in the office. Rushing to catch up on emails, the legitimate CFO emailed the bank with wire instructions, account numbers and amounts.
3. Once the request was received, the banker informed the CFO of the bank's wire transfer protocols and that additional security steps needed to be taken.
4. The CFO emailed the fraudster posing as the CEO and informed them of the bank's policy. The CEO then emailed the banker to authorize the wire and stressed the importance of getting the wire completed before the bank's cut off time of 2:00 PM.
5. In the email to the banker, the fraudulent CEO used uncommon words such as "kindly" and a date format of 13/7/2021.
6. The banker called the company to inform them of their suspicions. The CEO confirmed the request was fraudulent.





Scheme #3

Internal Fraud/Embezzlement

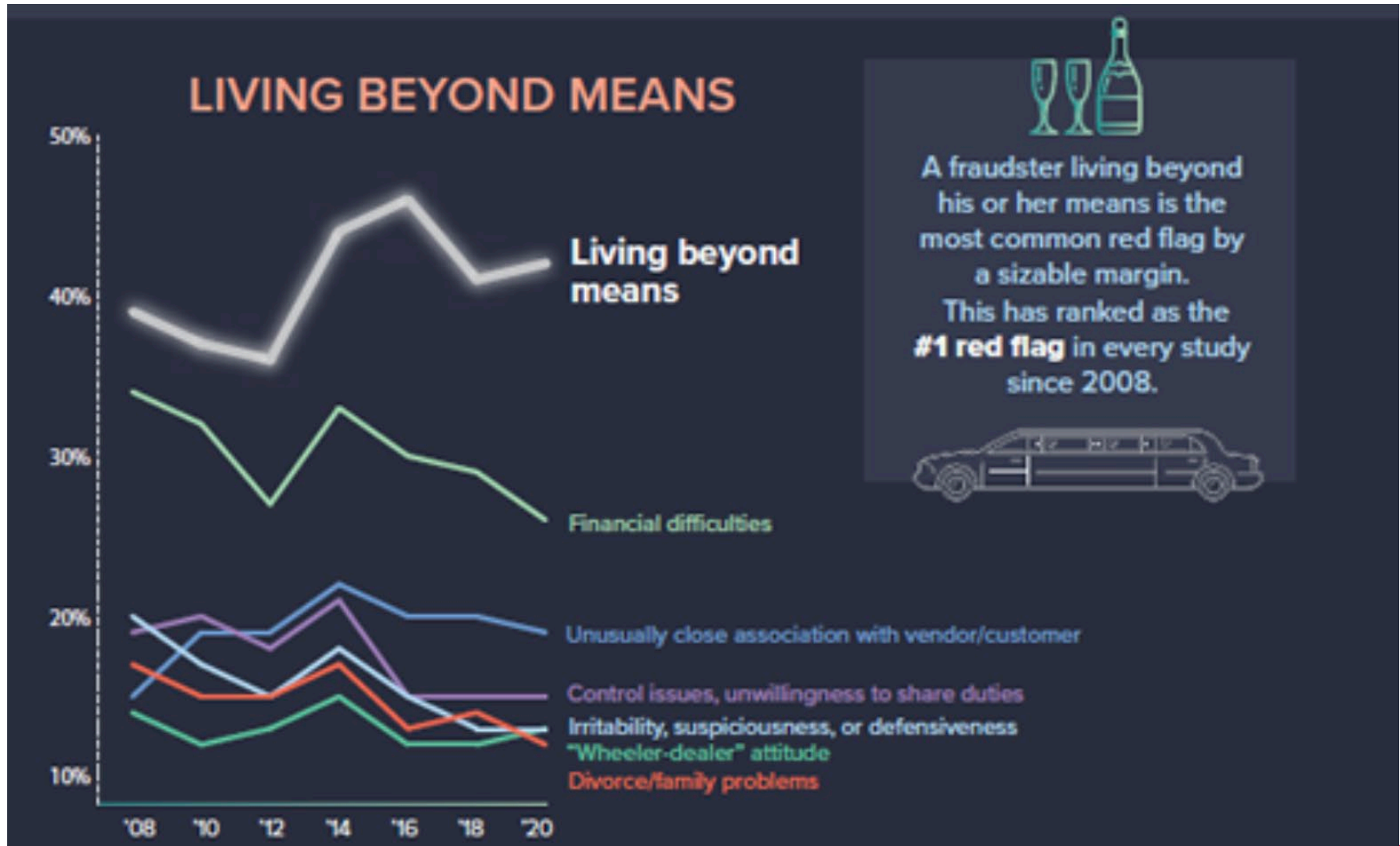


Internal Fraud/Embezzlement Statistics

- The median loss caused by occupational fraud was \$125,000, with 21% of cases causing losses of over \$1 million
- 70% of frauds occurred in for-profit organizations, with 26% being public entities.
- Most occupational fraud perpetrators are first-time offenders with clean employment histories.
- Approximately 86% had never been punished or terminated for fraud-related conduct by previous employers.
- The typical occupational fraud scheme lasts 14 months before it is detected and causes a loss of \$8,300 per month.



85% of fraud perpetrators displayed behavioral red flags that are often associated with fraudulent conduct





Internal Fraud/Embezzlement

A Case Study:

Rita Crundwell, Comptroller for the City of Dixon Illinois



- Crundwell began her work at the City of Dixon, Illinois in 1970 as part of a work study program while in high school. She was appointed comptroller in 1983.
- Outside of her work, Rita had a passion for softball, playing softball for the team of Clifton Gunderson (Dixon's independent audit firm at the time). Rita also pursued an interest in breeding and showing horses
- Crundwell built the first horse stables in 1997. Her ranch produced 52 world championship. Her salary at the time was approximately \$20,000.
- In 2000, she undertook a major expansion to the house, doubling the living space to nearly 3,500 square feet. She also built a nearly 20,000- square-foot horse barn in 2006 on another 88-acre property in the area
- She was allowed to work remotely for 3 months out of the year, having access to the cities email and calling in every day.
- In the early 2000's, the City of Dixon began to face financial difficulties. Crundwell pointed blame to State of Illinois and claimed that the city's hard times were due to nonpayment by the state



How did she do it?

84/08/2012 17:08 18157284500
03/21/2012 12:16 3135561295
Document #: 65-1 Filed: 02/13/13 Page 2 of 33
FBI LEGAL OPERATIONS 12:08:19 03-

815 284 4069 53 bank

SIGNATURE CARD

FIFTH THIRD BANK

OVERSICKE REFERENCE TO AS "BANK"

Name (Primary Owner) [Redacted] Account No. — RSCDA Reserve Fund
City of Dixon, IL Type
Street Address 113 West Second Street, PO Box 386
City and State Dixon, IL Zip 61021-0386
Home Phone 815-288-1485 Date of Birth 1-10-53 Mother's Maiden Name Schick
Employer CITY OF DIXON Work Phone 815-288-1485
Tax ID or S.S. Number _____ NEW ☐ ADD ☒ REPL
Ownership ☐ Joint ☐ Sole ☐ Partnership for Profit ☐ LLC ☐ Government Trust ☐ Non Profit (501(c)(3)) Other _____
*Joint accounts may be owned as joint tenants with right of survivorship, not as tenancy by the entirety.
*Corporation for Profit ☐ Non Resident Alien ☐ Sole Proprietorship ☐ Partnership for Profit ☐ LLC ☐ Government Trust ☐ Non Profit (501(c)(3)) Other _____
*Each Non Resident Alien must complete a W-9 Form
THE UNDERSIGNED AGREES TO THE TERMS AND CONDITIONS AT THE RIGHT

Title: Comptroller/Treasurer

Non-US Person*	Senior Foreign Officer**
Yes No Yes No	Yes No Yes No
Yes No Yes No	Yes No Yes No
Yes No Yes No	Yes No Yes No
Yes No Yes No	Yes No Yes No

Payable on Cash Beneficiary PO BOX 386, DIXON, IL 61021

USA PATRIOT ACT REQUIREMENTS:
*1. Are you a Non-US person with more than \$500,000 on deposit or account with Fifth Third?
*2. Are you a Senior Foreign Officer of a government, foreign military branch, political party, foreign government-owned company, or a foreign person or professional associated with one of these?
Under penalties of perjury, I certify that:
1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me).
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding.
3. I am a U.S. citizen or other U.S. person.
Certification Instructions - You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because of underreporting interest or dividends on your tax return.
Sign [Signature] Date 6/20/11
90-213 (5-07 REV 01/05) Send original to Check Processing IMCC11

Signature Card

Case: 3:12-cr-50027 Document #: 65-1 Filed: 02/13/13 Page 4 of 33 PageID #: 517
JUN-12-2012 11:22AM FROM: T-214 P.002/003 F-002

RESOLUTION OF CORPORATION AUTHORIZING OFFICERS TO MAKE DEPOSITS AND WITHDRAWALS

I HEREBY CERTIFY, that I am Secretary of the Board of Directors of City of Dixon of Dixon, Illinois a corporation organized and existing under the laws of the State of Illinois

I FURTHER CERTIFY, that a meeting of the Board of Directors of said Corporation was duly called and held at its office in the City of _____ and State of _____ on the _____ day of _____ 19____, that at said meeting a quorum was present and voting throughout, and that the following resolutions were duly adopted and are now in full force and effect.

RESOLVED, that First Bank South Bank Name and Address be and it is hereby designated as a depository of the funds of this Corporation, and that the said funds be subject to withdrawal upon checks, notes, drafts, bills of exchange, acceptances, undertakings or other orders for the payment of money when signed by: Rita Crundwell Only.

RESOLVED, that above named Bank is authorized to pay any such checks, notes, drafts, bills of exchange, acceptances, undertakings or other orders and also to receive the same for the credit of or in payment from the payee or any other holder without inquiry as to the circumstances of issue or the disposition of the proceeds thereof, even if drawn to the individual order of any signing officer or payable to said Bank or others for his account, or tendered in payment of his individual obligation.

RESOLVED, that any and all endorsements for or on behalf of this Corporation upon checks, drafts, notes or instruments for deposit or collection made with the said Bank may be written or stamped endorsements of the Corporation without any designation of the person making such endorsements.

RESOLVED, that said Bank be promptly notified in writing by the Secretary or any other officer of this Corporation of any change in these resolutions or our by-laws and that until it has actually received such notice in writing said Bank is authorized to act in pursuance of these resolutions.

I FURTHER CERTIFY, that these resolutions are within the power of the Board of Directors to pass as provided in the Charter and By-Laws of this Corporation, and that this Corporation and their respective titles are as follows:

Name _____ Title _____
Name _____ Title _____
Name _____ Title _____
Name _____ Title _____
Name _____ Title _____

IN WITNESS WHEREOF, I have hereunto set my hand as Secretary seal this 6th day of October 19 93

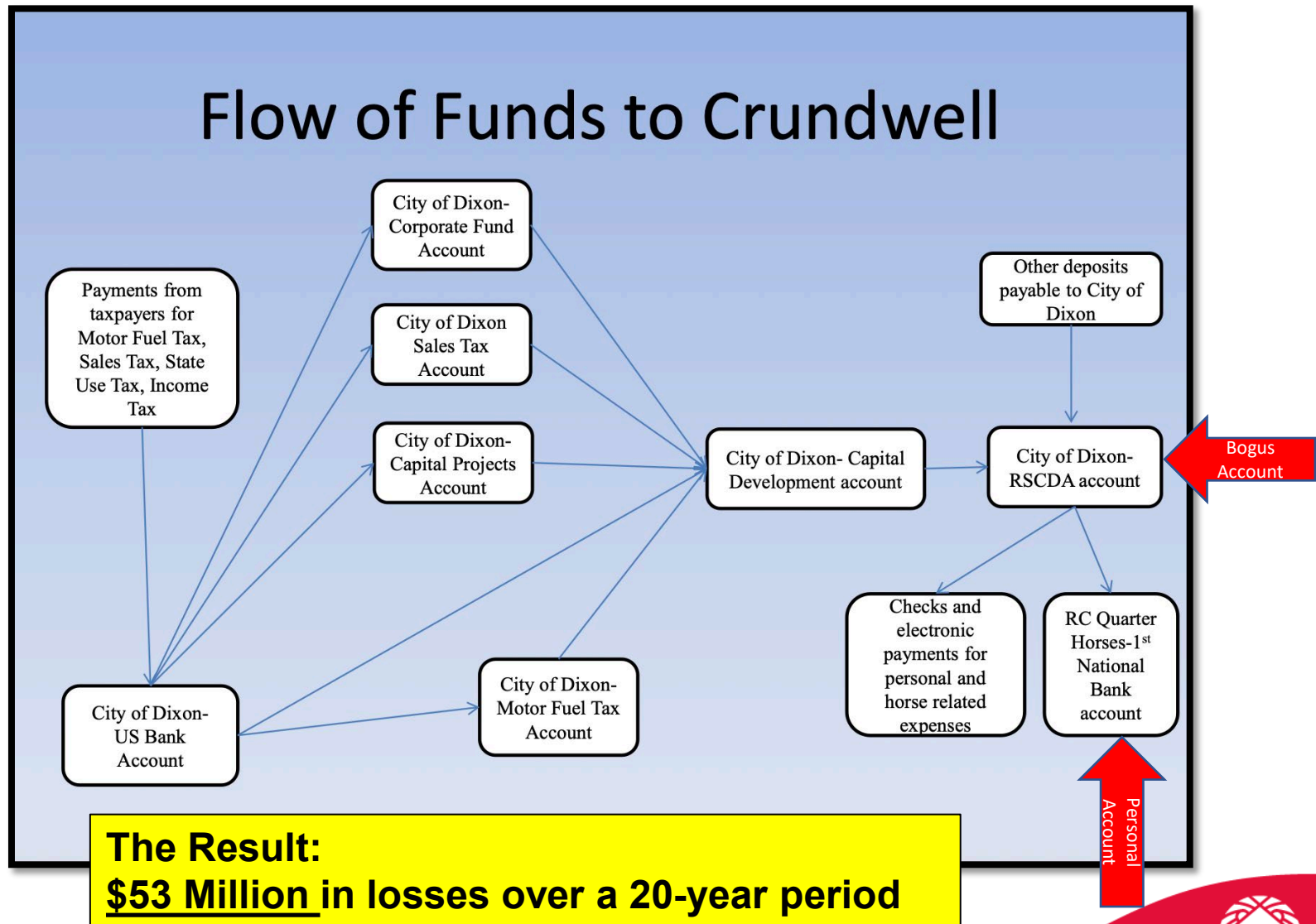
(Seal) [Signature]
Secretary of the Board of Directors
City of Dixon, Illinois

Corporate Resolution

Crundwell, alone, was allowed to sign checks and make withdrawals from RSCDA account



- Crundwell funneled money into the Capital Development Fund that she then transferred to the secret RSCDA account.





Scheme #4: Ransomware

- Ransomware perpetrators carry out more than 4,000 attacks daily.
- On average, organizations pay a ransom of \$233,217.
- There's a 19-day downtime following a ransomware attack.
- 95 new ransomware classification families were discovered in 2019 alone.
- Ransomware attacks rose by 388% between Q2 and Q3 of 2020, occurring every 11 seconds.
- The global cost associated with ransomware recovery will exceed \$20 billion in 2021



Ransomware

- Fraudster demands ransom to remove the restrictions
- Some forms systematically encrypt files on the system's hard drive.
- Difficult or impossible to decrypt without paying the ransom for the decryption key; some may simply lock the system and display messages to coax the user into paying
- Most Ransomware enters the system through attachments to an email message.





A Real-Life Example: Forward Air Trucking and Logistical Company

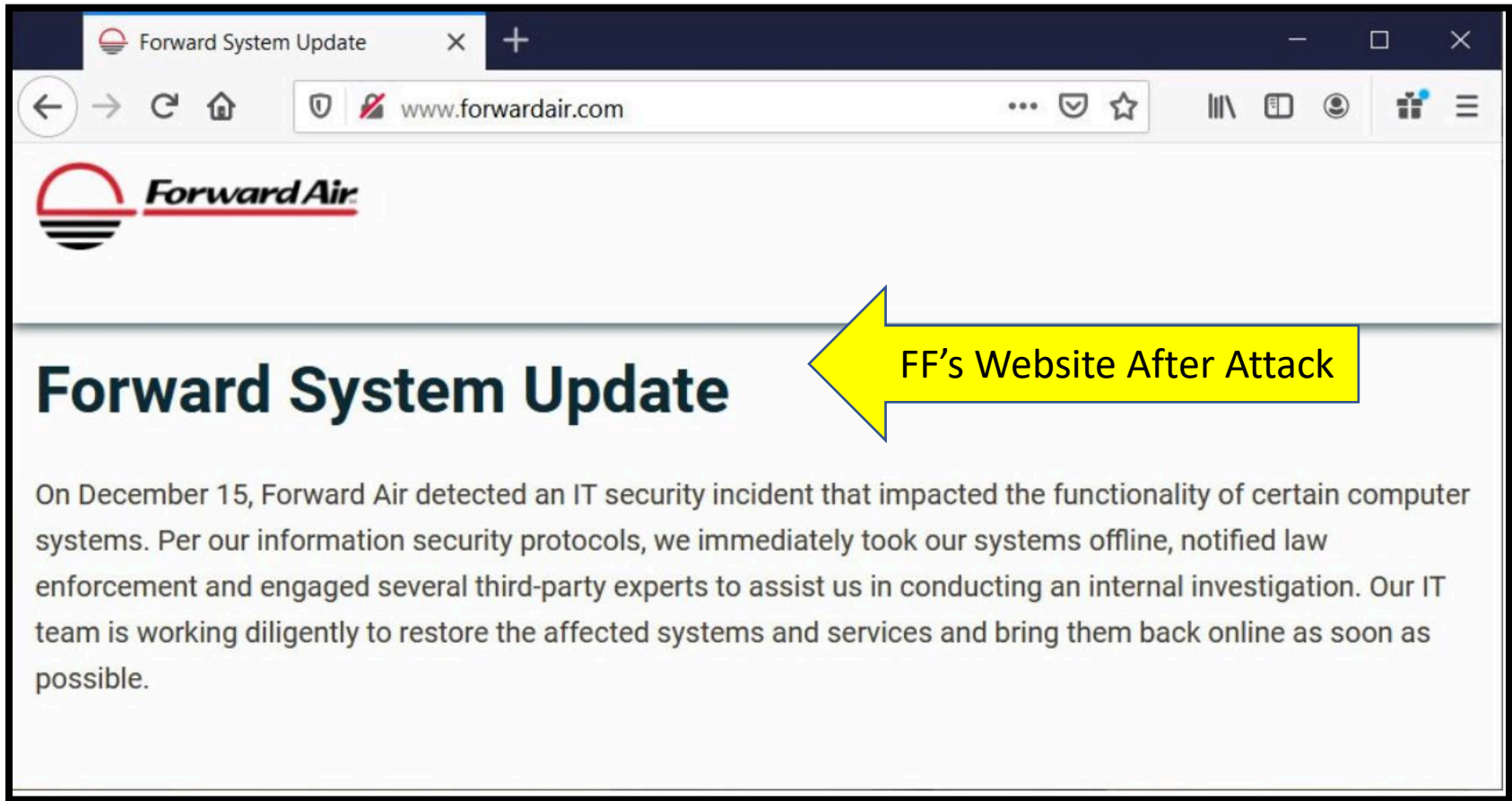


Ransomware: A Real Life Example

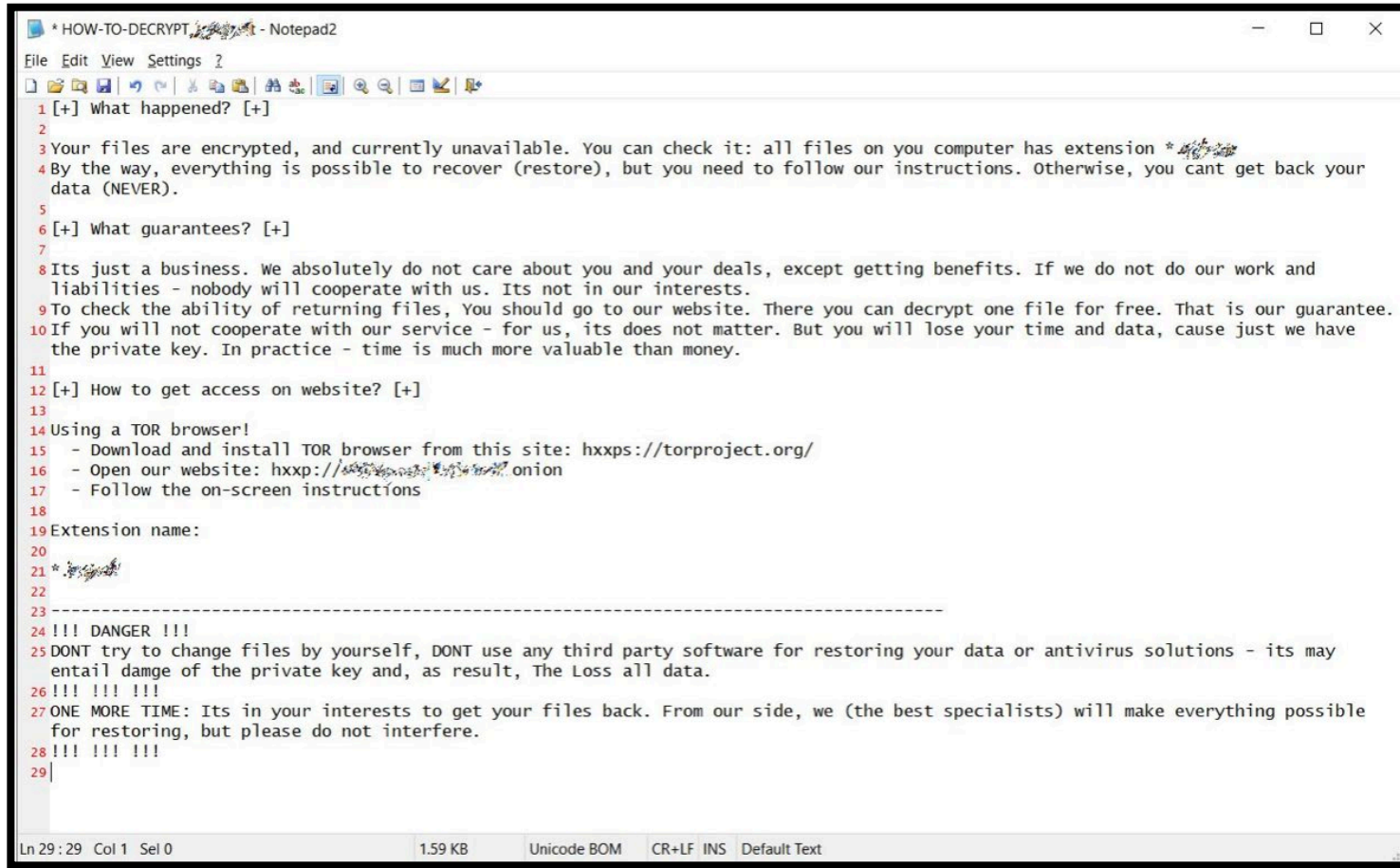
- On December 15 of 2020, Forward Air detected an IT security incident that impacted the functionality of certain computer systems. Later, it was discovered that the attack was a ransomware incident which was linked to the [Hades ransomware](#).
- Immediately after the attack, Forward Air took their systems offline. This resulted in freight forwarders and airlines scrambling to locate freight, book loads and find other ways to communicate with Forward Air.
- Drivers and employees were barred from accessing necessary documents and transport requirements
- The attack left a dent of \$7.5 million in its Q4 financial results



Ransomware



Ransomware



```
* HOW-TO-DECRYPT - Notepad2
File Edit View Settings ?
1 [+] What happened? [+]
2
3 Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension *.xxx
4 By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant get back your
  data (NEVER).
5
6 [+] What guarantees? [+]
7
8 Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and
  liabilities - nobody will cooperate with us. Its not in our interests.
9 To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
10 If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have
   the private key. In practice - time is much more valuable than money.
11
12 [+] How to get access on website? [+]
13
14 Using a TOR browser!
15 - Download and install TOR browser from this site: hxxps://torproject.org/
16 - Open our website: hxxp://xxx.onion
17 - Follow the on-screen instructions
18
19 Extension name:
20
21 *.xxx
22
23 -----
24 !!! DANGER !!!
25 DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may
  entail damge of the private key and, as result, The Loss all data.
26 !!! !!! !!!
27 ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) will make everything possible
  for restoring, but please do not interfere.
28 !!! !!! !!!
29
```

- Fraudster demands ransom to remove the restrictions
- Some forms systematically encrypt files on the system's hard drive.
- Difficult or impossible to decrypt without paying the ransom for the decryption key; some may simply lock the system and display messages to coax the user into paying
- Most Ransomware enters the system through attachments to an email message.

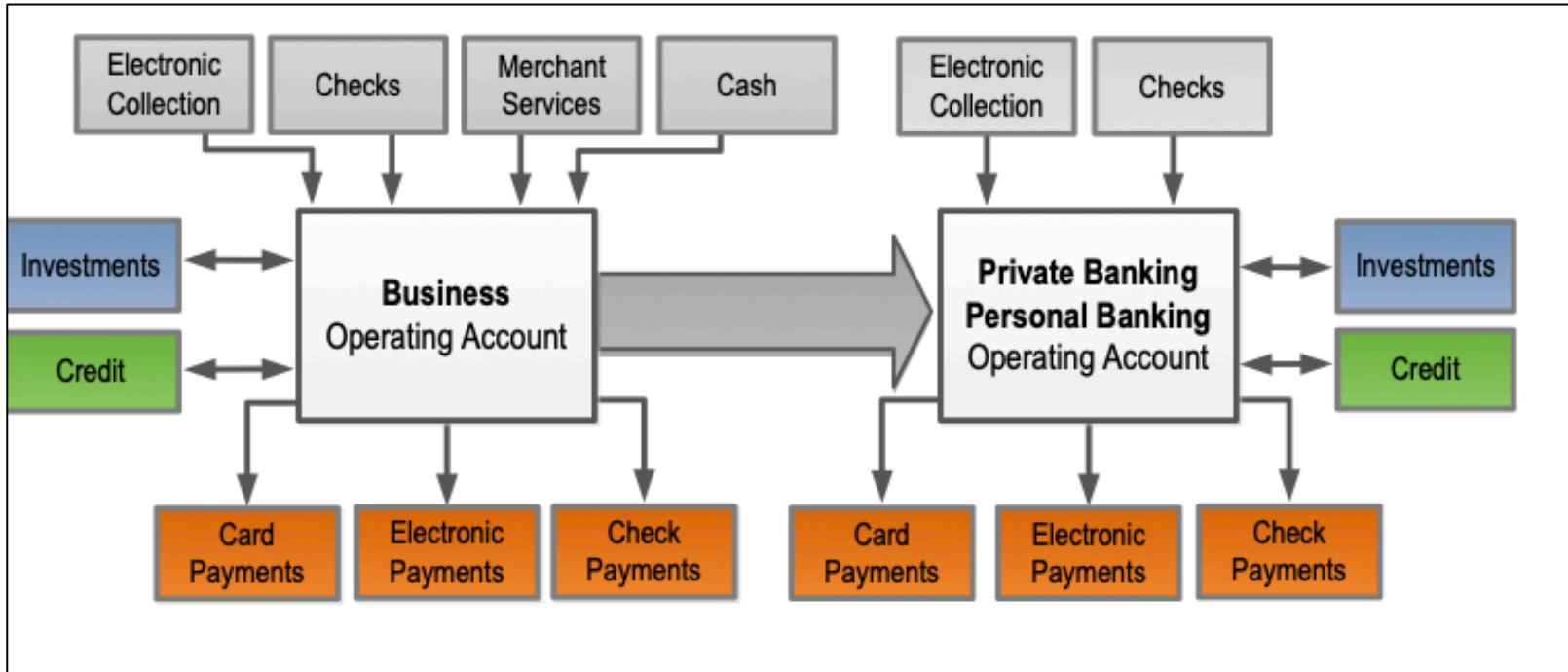


Tips on How to Safeguard Your Financial Assets

- **Be careful with what information you share online or on social media.** By openly sharing things like pet names, schools you attended, links to family members, and your birthday, **you can give a scammer all the information they need to guess your password** or answer your security questions.
- **Don't click on anything in an unsolicited email or text message** asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate
- **Carefully examine the email address, URL, and spelling used in any correspondence.** Scammers use slight differences to trick your eye and gain your trust.
- **Verify payment and purchase requests** in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request. Be especially wary if the requestor is pressing you to act quickly.
- **Implement Dual Controls.** Ensure there are systems of checks and balances in place.
- **Conduct all online banking activities from a standalone, hardened and completely locked down computer.**
 - Regularly review user access
 - Implement dual controls
 - Establish company and user entitlement limits
 - Review full transaction details before releasing the funds
 - Reconcile account activity daily
 - Set up email alerts for ACH, wire and balance thresholds
 - Never write down passwords, usernames or token passwords
 - Verify payment instructions and details
- **Avoid writing checks whenever possible**



Review your County's Cash Cycle





About Ameris

- Founded in 1971 as American Banking Company
- In 1996, we expanded into the state of Alabama with the acquisition of Southland Bank.
- In July of 2019, Ameris completed the merger with Fidelity Bank creating a combined company has over \$18 billion in assets and a branch network across five states
- The Ameris Approach was deployed, so that as Ameris Bank continues to grow, our founding principles of high-performance solutions, character and community will always shine through

**FOUNDED IN 1971 AS AMERICAN
BANKING COMPANY**

**LOCATIONS THROUGHOUT
ALABAMA, FLORIDA, GEORGIA,
SOUTH CAROLINA AND NORTH
CAROLINA**

**GROWTH STRATEGY OF ACQUIRING
BANKS IN COMMUNITIES
THROUGHOUT OUR FOOTPRINT**

**IN 1987, FIRST PUBLIC STOCK
OFFERING**

**IN 2006, MULTI-CHARTER COLLAPSE
OF ALL INSTITUTIONS INTO ONE
SINGLE BRAND – AMERIS BANK**

**PUBLICALLY TRADED ON THE
NASDAQ UNDER ABCB**

For More Information, Contact:

Kevin Strickland

Director of Nonprofit and Association Banking

kevin.strickland@amerisbank.com

850-661-3972

