Welcome

Treasury Management Security Forum

Thank you for your patience. The presentation will begin shortly.

Forum Agenda

- Modern Security Threats
- Fraud Prevention and Detection
- Treasury Management Security
- Panel Discussion and Q&A

Modern Security Threats

Josh Pierce – Security Architect

FirstBank’s Security Team

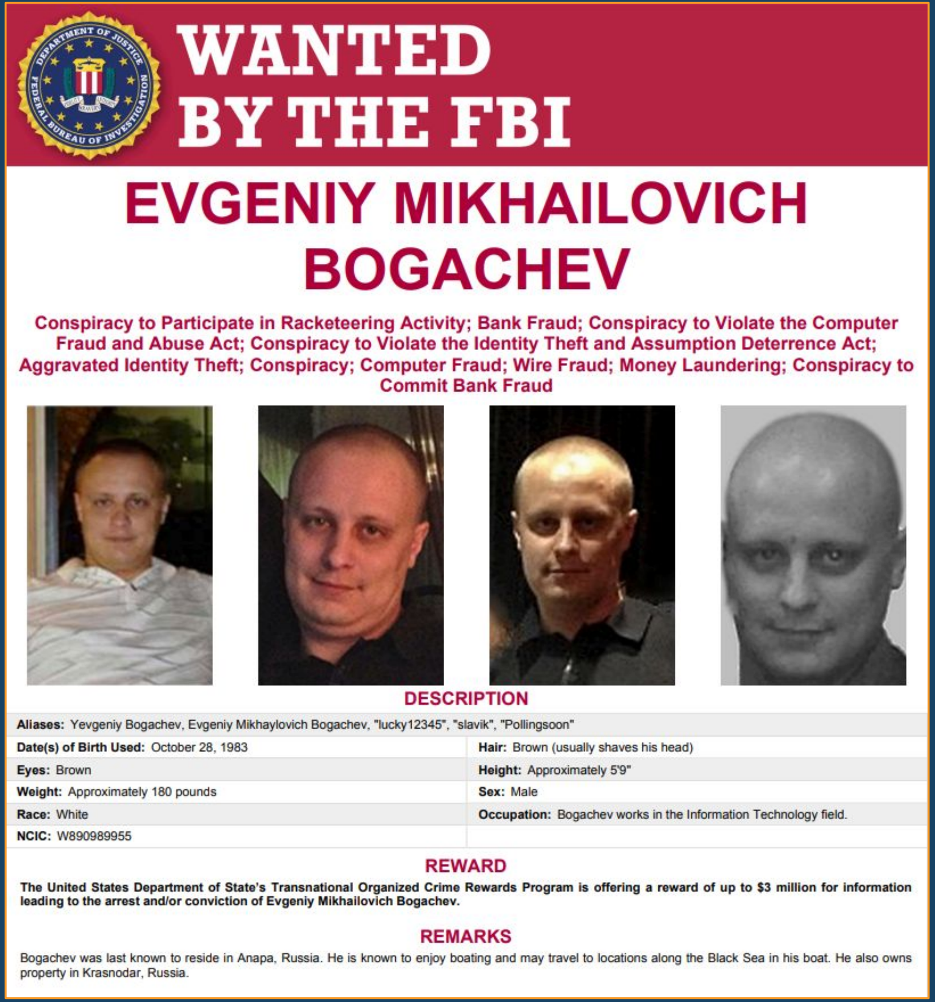
- 50+ highly-trained employees dedicated to security
- Expert staff who are highly regarded in the industry
- Industry-leading technologies and security controls
- Focused on securing FirstBank and protecting customers

2024 Attack Landscape

- 30,458 security incidents with 10,626 data breaches were analyzed in Verizon’s Data Breach Incident Report
- 68% of breaches include a “human element”
  - Errors, credential theft via social engineering (privilege misuse removed this year)
- 90%+ of breaches are financially driven and any target can be profitable
- 32% of breaches involved ransomware or extortion

Why are attackers still so effective?

В216ОР 777 RUS
В215ОР 777 RUS
В216ОР 777 RUS
Н644ТН 777
В216ОР 777
В215ОР 777



WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

REMARKS

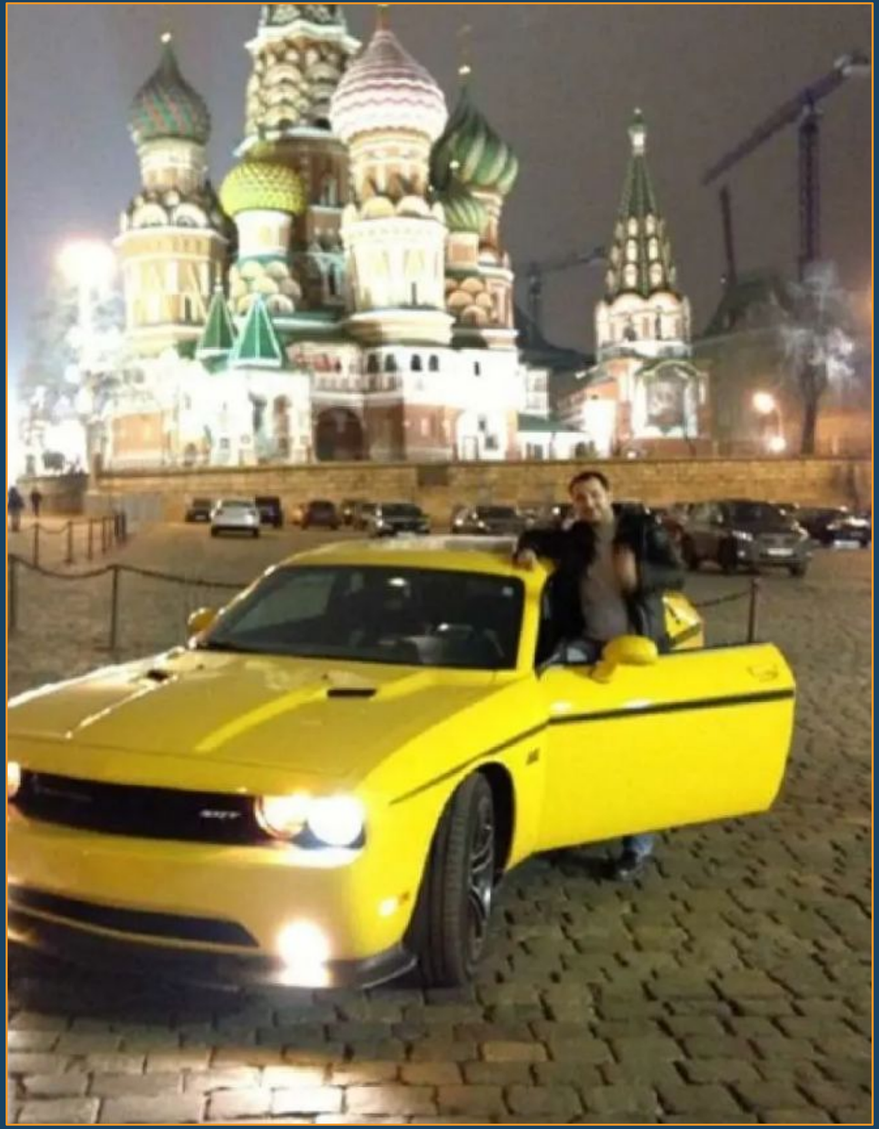
Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

"What a talented guy," said Mikhail, who regularly sees him around the city. "Sitting at his computer at home, he broke into our enemies' camp, but did not harm his fellow Russians."

“While Mr. Bogachev was draining bank accounts, it appears that the Russian authorities were looking over his shoulder, searching the same computers for files and emails. In effect, they were grafting an intelligence operation onto a far-reaching cybercriminal scheme, sparing themselves the hard work of hacking into the computers themselves, officials said.”

– New York Times

- Hacked Target & Neiman Marcus
- $170 million in losses
- 3,700 victimized banks
- 500 victimized businesses
- Arrested in Maldives!

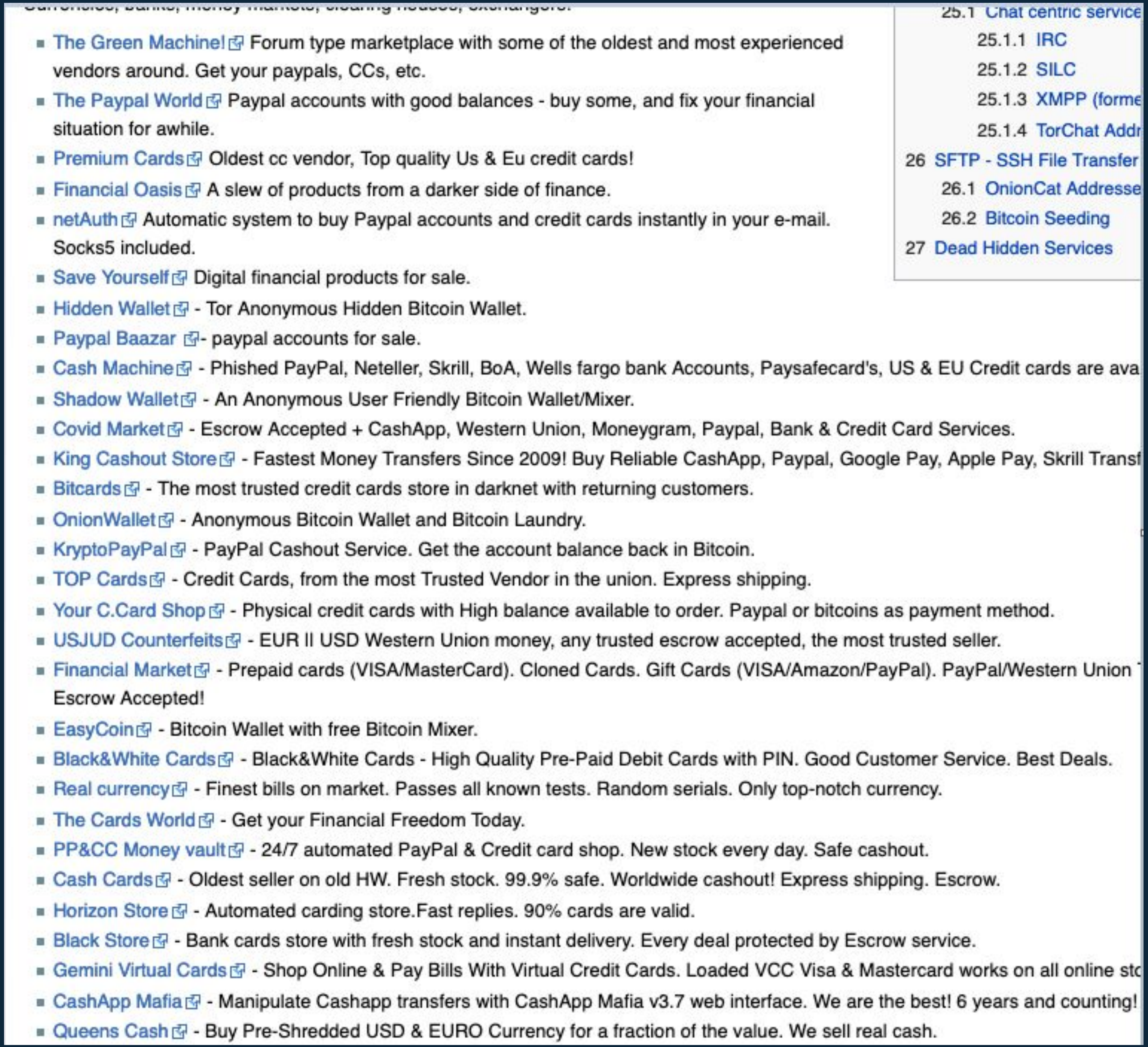


Why are attackers still so effective?

- Sophisticated organized crime groups
- Function like corporations:
  - HR
  - Hiring
  - Legal Counsel
  - Recruiters
- Significant funding and low risk

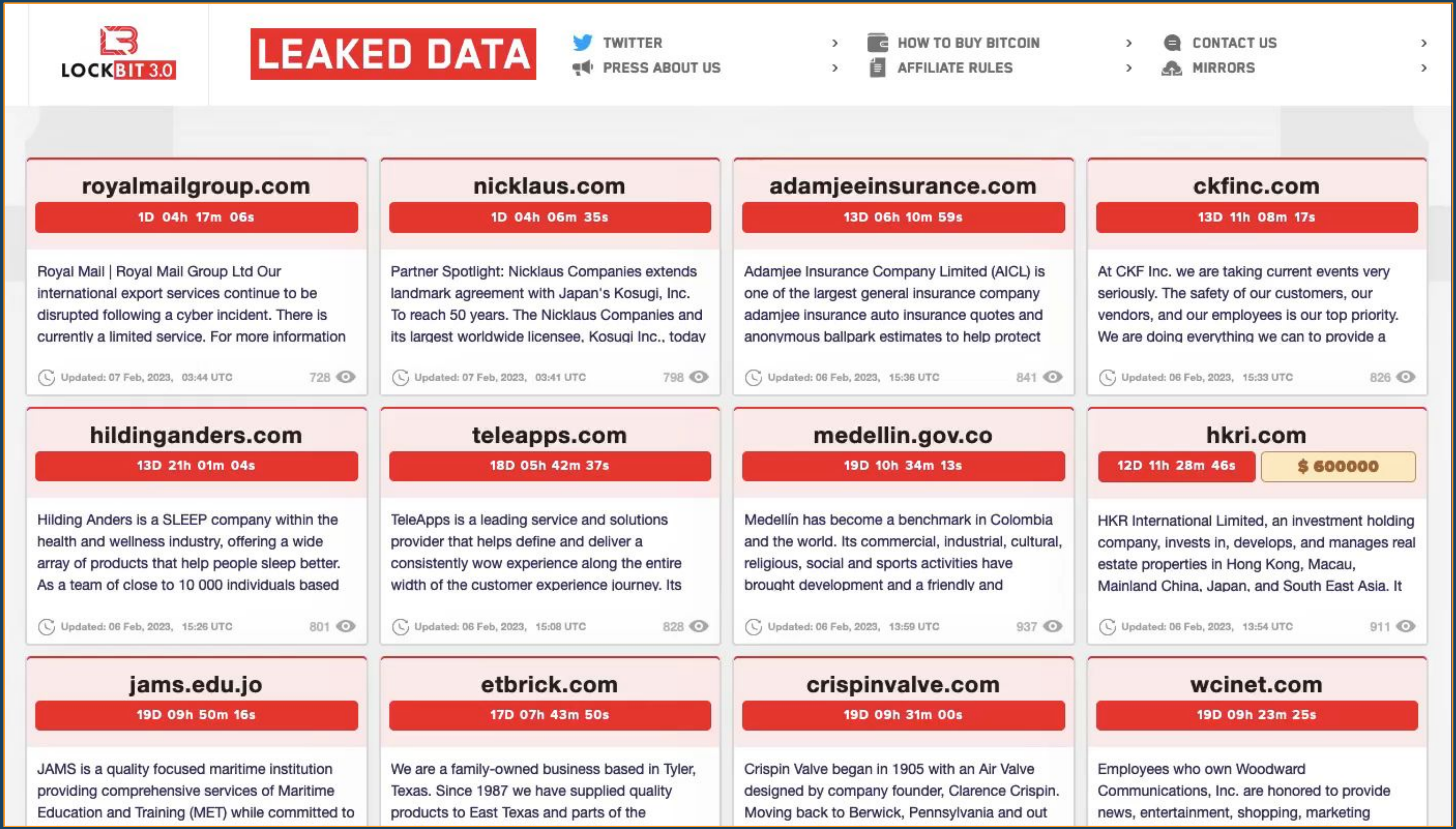
How does the “Dark Web” play a role?

- Ransomware actors utilize the Dark Web for a lot of their infrastructure.
- RaaS
- Monetization
- Support, Collaboration, Training



Currencies, banks, money markets, clearing houses, exchangers:

- The Green Machine! Forum type marketplace with some of the oldest and most experienced vendors around. Get your paypals, CCs, etc.
- The Paypal World Paypal accounts with good balances - buy some, and fix your financial situation for awhile.
- Premium Cards Oldest cc vendor, Top quality Us & Eu credit cards!
- Financial Oasis A slew of products from a darker side of finance.
- netAuth Automatic system to buy Paypal accounts and credit cards instantly in your e-mail. Socks5 included.
- Save Yourself Digital financial products for sale.
- Hidden Wallet - Tor Anonymous Hidden Bitcoin Wallet.
- Paypal Baazar - paypal accounts for sale.
- Cash Machine - Phished PayPal, Neteller, Skrill, BoA, Wells fargo bank Accounts, Paysafecard's, US & EU Credit cards are ava
- Shadow Wallet - An Anonymous User Friendly Bitcoin Wallet/Mixer.
- Covid Market - Escrow Accepted + CashApp, Western Union, Moneygram, Paypal, Bank & Credit Card Services.
- King Cashout Store - Fastest Money Transfers Since 2009! Buy Reliable CashApp, Paypal, Google Pay, Apple Pay, Skrill Transf
- Bitcards - The most trusted credit cards store in darknet with returning customers.
- OnionWallet - Anonymous Bitcoin Wallet and Bitcoin Laundry.
- KryptoPayPal - PayPal Cashout Service. Get the account balance back in Bitcoin.
- TOP Cards - Credit Cards, from the most Trusted Vendor in the union. Express shipping.
- Your C.Card Shop - Physical credit cards with High balance available to order. Paypal or bitcoins as payment method.
- USJUD Counterfeits - EUR II USD Western Union money, any trusted escrow accepted, the most trusted seller.
- Financial Market - Prepaid cards (VISA/MasterCard). Cloned Cards. Gift Cards (VISA/Amazon/PayPal). PayPal/Western Union Escrow Accepted!
- EasyCoin - Bitcoin Wallet with free Bitcoin Mixer.
- Black&White Cards - Black&White Cards - High Quality Pre-Paid Debit Cards with PIN. Good Customer Service. Best Deals.
- Real currency - Finest bills on market. Passes all known tests. Random serials. Only top-notch currency.
- The Cards World - Get your Financial Freedom Today.
- PP&CC Money vault - 24/7 automated PayPal & Credit card shop. New stock every day. Safe cashout.
- Cash Cards - Oldest seller on old HW. Fresh stock. 99.9% safe. Worldwide cashout! Express shipping. Escrow.
- Horizon Store - Automated carding store.Fast replies. 90% cards are valid.
- Black Store - Bank cards store with fresh stock and instant delivery. Every deal protected by Escrow service.
- Gemini Virtual Cards - Shop Online & Pay Bills With Virtual Credit Cards. Loaded VCC Visa & Mastercard works on all online stc
- CashApp Mafia - Manipulate Cashapp transfers with CashApp Mafia v3.7 web interface. We are the best! 6 years and counting!
- Queens Cash - Buy Pre-Shredded USD & EURO Currency for a fraction of the value. We sell real cash.



royalmailgroup.com

1D 04h 17m 06s

Royal Mail | Royal Mail Group Ltd Our international export services continue to be disrupted following a cyber incident. There is currently a limited service. For more information

Updated: 07 Feb, 2023, 03:44 UTC 728

nicklaus.com

1D 04h 06m 35s

Partner Spotlight: Nicklaus Companies extends landmark agreement with Japan's Kosugi, Inc. To reach 50 years. The Nicklaus Companies and its largest worldwide licensee, Kosugi Inc., today

Updated: 07 Feb, 2023, 03:41 UTC 798

adamjeeinsurance.com

13D 06h 10m 59s

Adamjee Insurance Company Limited (AICL) is one of the largest general insurance company adamjee insurance auto insurance quotes and anonymous ballpark estimates to help protect

Updated: 06 Feb, 2023, 15:36 UTC 841

ckfinc.com

13D 11h 08m 17s

At CKF Inc. we are taking current events very seriously. The safety of our customers, our vendors, and our employees is our top priority. We are doing everything we can to provide a

Updated: 06 Feb, 2023, 15:33 UTC 826

hildinganders.com

13D 21h 01m 04s

Hilding Anders is a SLEEP company within the health and wellness industry, offering a wide array of products that help people sleep better. As a team of close to 10 000 individuals based

Updated: 06 Feb, 2023, 15:26 UTC 801

teleapps.com

18D 05h 42m 37s

TeleApps is a leading service and solutions provider that helps define and deliver a consistently wow experience along the entire width of the customer experience journey. Its

Updated: 06 Feb, 2023, 15:08 UTC 828

medellin.gov.co

19D 10h 34m 13s

Medellín has become a benchmark in Colombia and the world. Its commercial, industrial, cultural, religious, social and sports activities have brought development and a friendly and

Updated: 06 Feb, 2023, 13:59 UTC 937

hkri.com

12D 11h 28m 46s $ 600000

HKR International Limited, an investment holding company, invests in, develops, and manages real estate properties in Hong Kong, Macau, Mainland China, Japan, and South East Asia. It

Updated: 06 Feb, 2023, 13:54 UTC 911

jams.edu.jo

19D 09h 50m 16s

JAMS is a quality focused maritime institution providing comprehensive services of Maritime Education and Training (MET) while committed to

etbrick.com

17D 07h 43m 50s

We are a family-owned business based in Tyler, Texas. Since 1987 we have supplied quality products to East Texas and parts of the

crispinvalve.com

19D 09h 31m 00s

Crispin Valve began in 1905 with an Air Valve designed by company founder, Clarence Crispin. Moving back to Berwick, Pennsylvania and out

wcinet.com

19D 09h 23m 25s

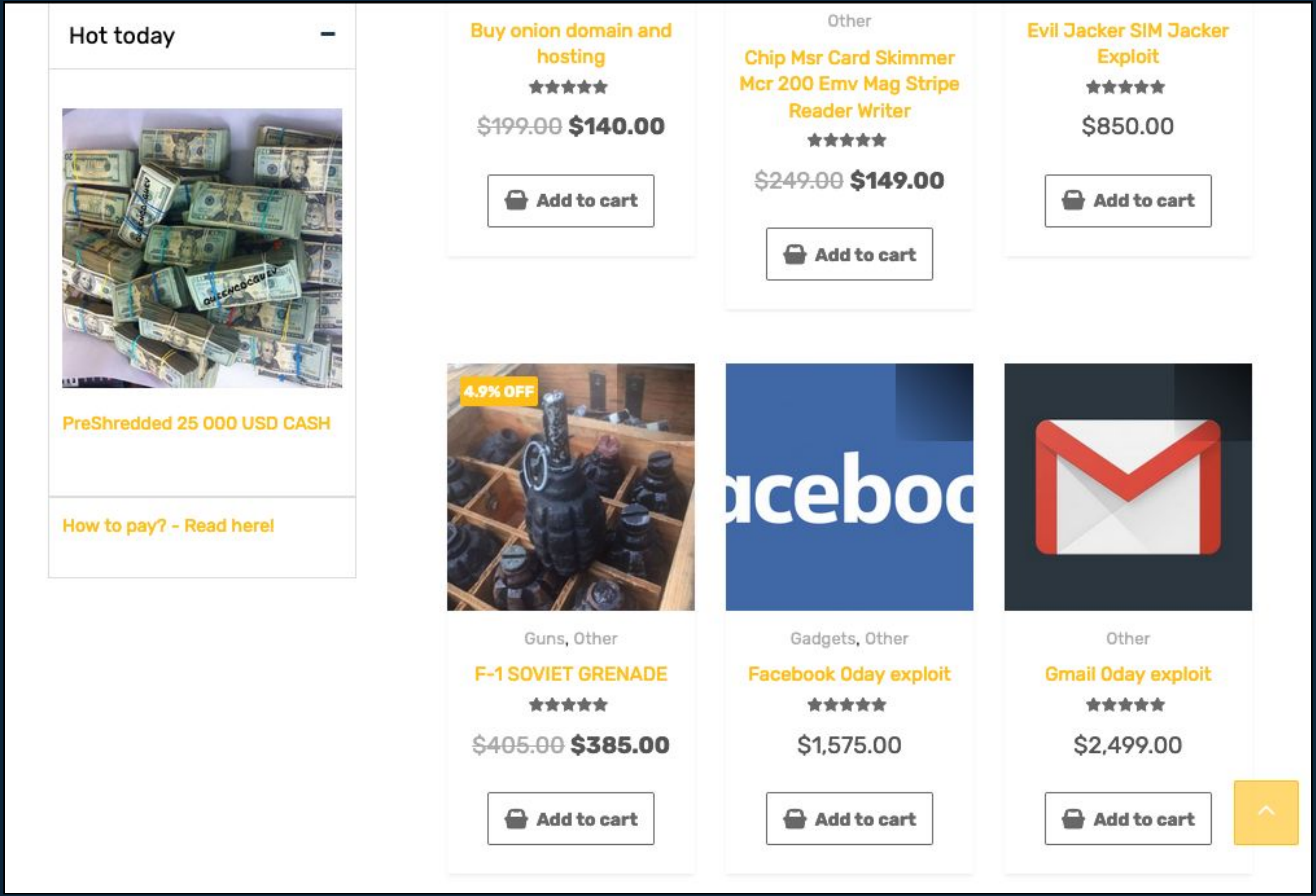
Employees who own Woodward Communications, Inc. are honored to provide news, entertainment, shopping, marketing

How does the “Dark Web” play a role?

- Crime as a service
- Organized crime vs. the “kid in mom’s basement”
- Any target that can be monetized will be
  - “We are too small to be a target.”

Empire Market

- Empire Market was one of the larger markets on the Dark Web. Here you could buy a wide variety of goods, from illegal drugs to exploits for software.
- In the following image you will see some goods for sale on Empire Market, including hand grenades and exploits for Facebook and Gmail.



Hot today

PreShredded 25 000 USD CASH

How to pay? - Read here!

Buy onion domain and hosting
★★★★★
~~$199.00~~ $140.00
Add to cart

Other
Chip Msr Card Skimmer Mcr 200 Emv Mag Stripe Reader Writer
★★★★★
~~$249.00~~ $149.00
Add to cart

Evil Jacker SIM Jacker Exploit
★★★★★
$850.00
Add to cart

4.9% OFF
Guns, Other
F-1 SOVIET GRENADE
★★★★★
~~$405.00~~ $385.00
Add to cart

Gadgets, Other
Facebook 0day exploit
★★★★★
$1,575.00
Add to cart

Other
Gmail 0day exploit
★★★★★
$2,499.00
Add to cart

Where should we focus?

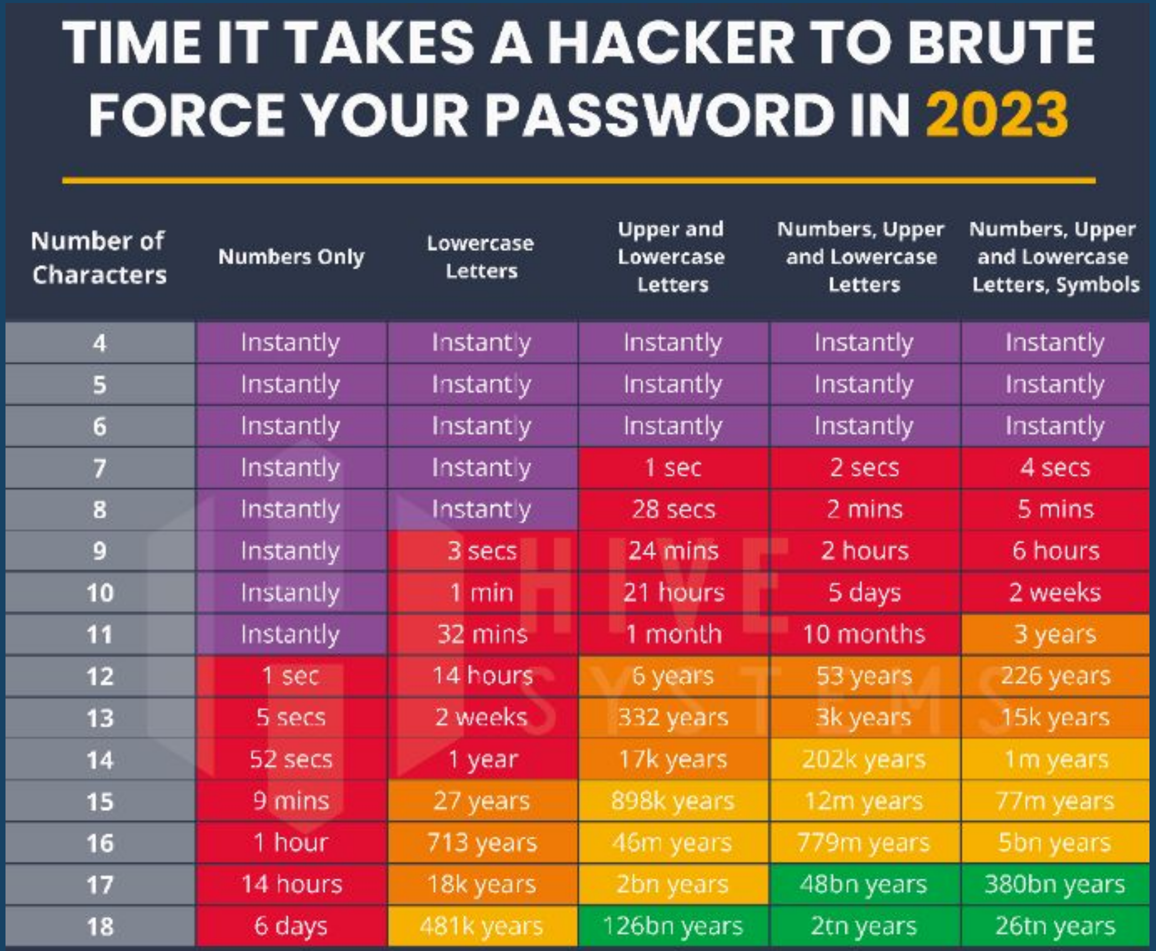
- Security and awareness training
- Data backups and recovery
- Principle of least privilege
- Insurance

Where should we focus?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/stopransomware

Where should we focus?



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

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

HIVE SYSTEMS

Source: hivesystems.io/password

Where should we focus?

Security Awareness and Training

- Password strength and storage
- Phishing
- Incident response
  - What is the plan when something goes wrong?
  - Who needs to know about an incident?
  - Who do we contact?
- Cyber hygiene
  - Anti-virus
  - Encryption
  - Patching

Where should we focus?

Data Backups and Recovery

- Maintain offline, encrypted backups of critical data
- Test the availability and integrity of backups
- Maintain backups offline
  - They will be a target
- Develop and practice exercising an incident response plan

Where should we focus?

Principle of Least Privilege

- Limit employee rights to only those necessary
- Restrict who has admin rights in your environment
- Can you restrict who can install software?
- How do we limit who has access to critical data?
- Think of data in terms of a “blast radius”

Where should we focus?

Insurance

- Every company should evaluate obtaining Cyber Insurance
- Ransomware:
  - Reduce financial harm
  - Breach Coach and Response Assistance
  - Best practice Incident Response processes
  - Notification Assistance
- Increasingly difficult and expensive to obtain
- Expect “audit like” questions and evaluations

Fraud Detection and Prevention

Bradley Champion – Director, Fraud Prevention

FirstBank's Fraud Prevention Team

- 20+ Representatives to provide customer support and transaction monitoring
- 7 highly trained Fraud Investigators who work more complex cases and perform recovery efforts
- 4 Data Analysts to analyze and respond to fraud trends

Check Fraud: Still Holding Strong

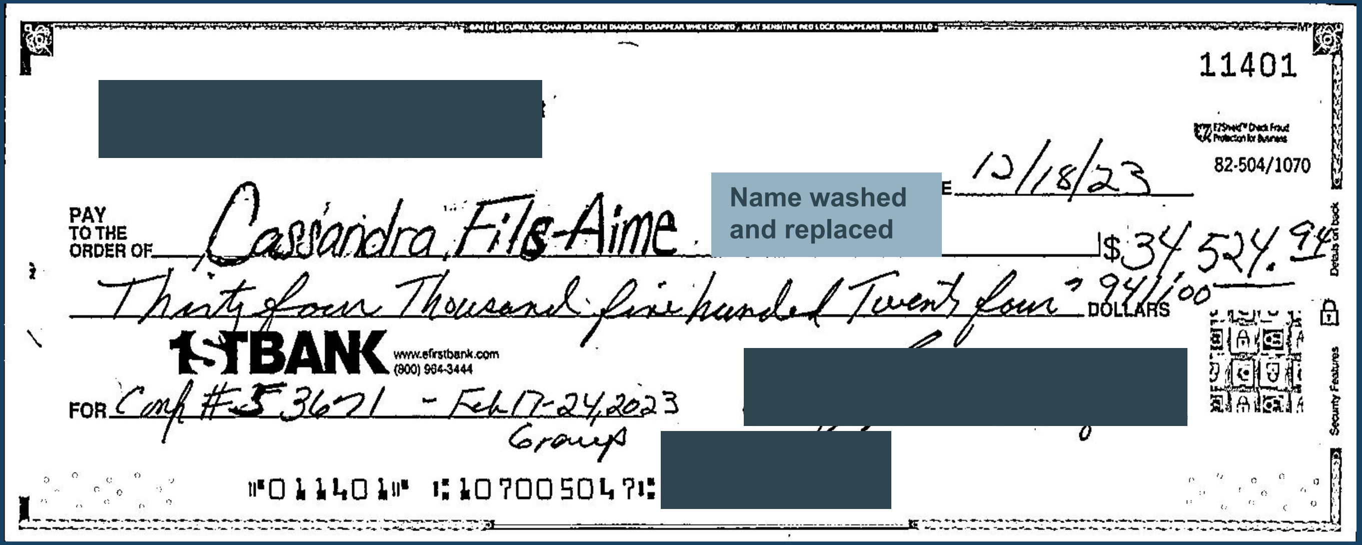
- Checks and Wires continue to be the two largest payment channels with reported fraud for commercial accounts.
- According to the 2024 AFP Payment Fraud report 65% of all respondents reported they were victims to check fraud.
- Year-to-date, 66% of check fraud reported at FirstBank is from commercial customers.

Check Fraud

- Check fraud has doubled and even tripled for some financial institutions over the past several years.
- Mail theft on the rise
  - USPS blue boxes – theft of arrow keys
  - Checks stolen out of cars (gyms and parks)
- Checks are then altered or counterfeited and negotiated by depositing into an account or cashed out at a branch location.

Altered Checks

- Original check is washed or manipulated to change the payee
  - Checks are being altered to add an additional name on top of the original payee's name. Adding "or" to the payee name and adding a 2nd person.



GREEN SECURELINK CHAIN AND GREEN DIAMOND DISAPPEAR WHEN COPIED / HEAT SENSITIVE RED LOCK DISAPPEARS WHEN HEATED

11401

[redacted]

F2Shield™ Check Fraud Protection for Business

82-504/1070

DATE 12/18/23

PAY TO THE ORDER OF Cassandra Fils-Aime $34,524.94

Name washed and replaced

Thirty four Thousand five hundred Twenty four 94/100 DOLLARS

1STBANK www.efirstbank.com (800) 964-3444

[redacted]

FOR Conf #536?1 - Feb 17-24, 2023 Group

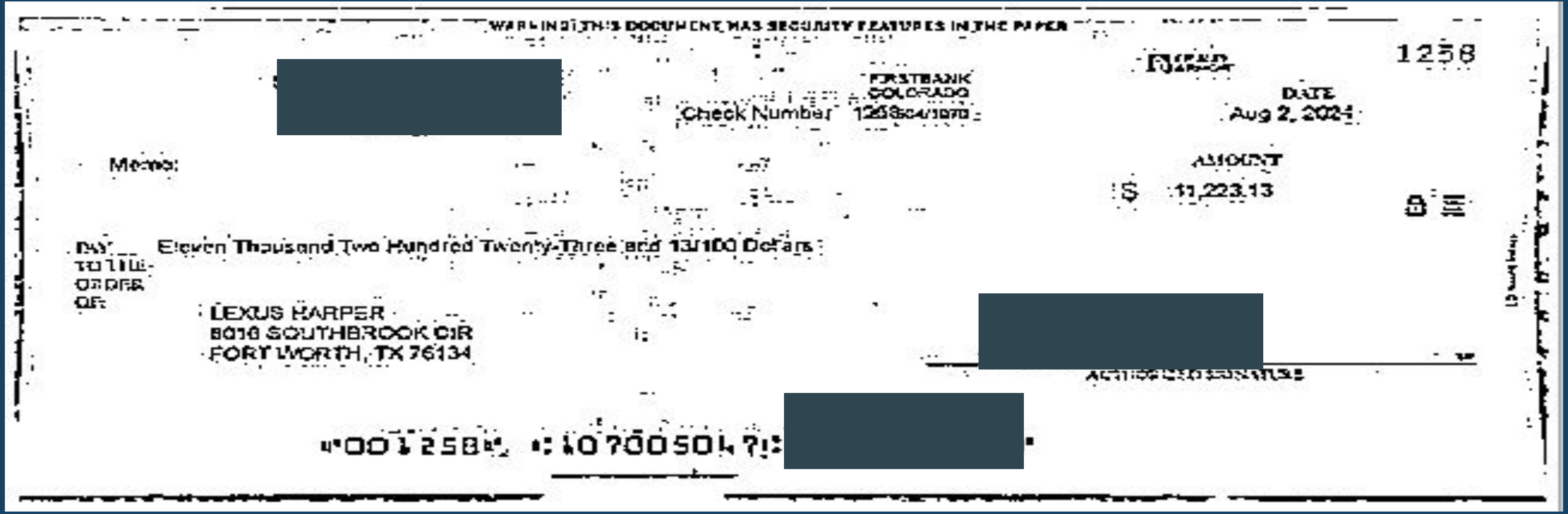
⑈011401⑈ ⑆107005047⑆ [redacted]

Details on back

Security Features

Counterfeit Checks

- Checks being used to create counterfeit checks using blank check stock.
- Check number and dollar amount matched, the payee name was different.
- Bookkeepers/Accountants typically only verify check # and dollar amount, however due to prevalence of altered and counterfeit checks, the payee name should also be verified.



WARNING: THIS DOCUMENT HAS SECURITY FEATURES IN THE PAPER

[redacted]

FIRSTBANK
COLORADO

Check Number 1258[illegible]

1258

DATE
Aug 2, 2024

Memo:

AMOUNT
$ 11,223.13

PAY Eleven Thousand Two Hundred Twenty-Three and 13/100 Dollars
TO THE
ORDER
OF:

LEXUS HARPER
8016 SOUTHBROOK CIR
FORT WORTH, TX 76134

[redacted]

AUTHORIZED SIGNATURE

⑈001258⑈ ⑆107005047⑆ [redacted]

business **banking for good** 1STBANK

Best Practices for Fighting Check Fraud

- Sign up for Positive Pay with payee verification
- Monitor your account activity on a daily basis
- Review check images on larger dollar checks
- Use a single check stock
- If you have to mail checks, drop them off inside the post office
- Use alternative payment methods (ACH, Bill Pay, Wire)
- Keep your checks in a secure location
- If at any time you discover a check cleared that you did not authorize, immediately contact FirstBank (303-237-5000; option 5 to reach Fraud Prevention)

Business Email Compromise (BEC)

- What is BEC?
  - Internal BEC
  - External BEC
- Best practices for fighting BEC
  - Call to verify any payment instructions at a trusted phone number
  - AI can be used; make sure you're talking to the right person
  - Utilize dual control for electronic payment methods

Business Email Compromise (BEC)

The fraudster

- Poses as a person or entity you know and trust.
- Requests a payment, submits an invoice or asks to change vendor payment instructions.
- Contacts you from an email that appears familiar.

! If you fall for the scam, any payments you send go to the fraudster — not where you intended.

Internal BEC

The fraudster

- Poses as your CEO, CFO, controller, or company owner.
- Emails you from an email address that appears consistent with prior emails.
- Asks you to send payments outside of normal process – typically by wire or ACH; often with urgency.
- May ask you to
  - Keep the payment confidential
  - Reply once you've sent payment

Internal BEC

What fraudsters hope to take advantage of

- Executive requests will not be questioned.
- Executives are often unavailable to verify requests.
- Urgent requests for money movement will not follow normal procedures.

External BEC

The fraudster

- Poses as vendor, supplier, or other business partner.
- Contacts you from an email that appears familiar.
- Asks for a payment via wire or ACH when check payment is typical.
- Asks to change their bank account information: "We need to receive payments to this new account."
- Sends an invoice that appears to be legitimate.

External BEC

What fraudsters hope to take advantage of

- Companies often change vendor bank account information based solely on an email that appears to be from the vendor.
- Companies often don't call back a trusted source at the vendor to authenticate a request.
- Companies often don’t have procedures in place to verbally verify payment changes to employees for payroll, or payments to vendors.

BEC is Different

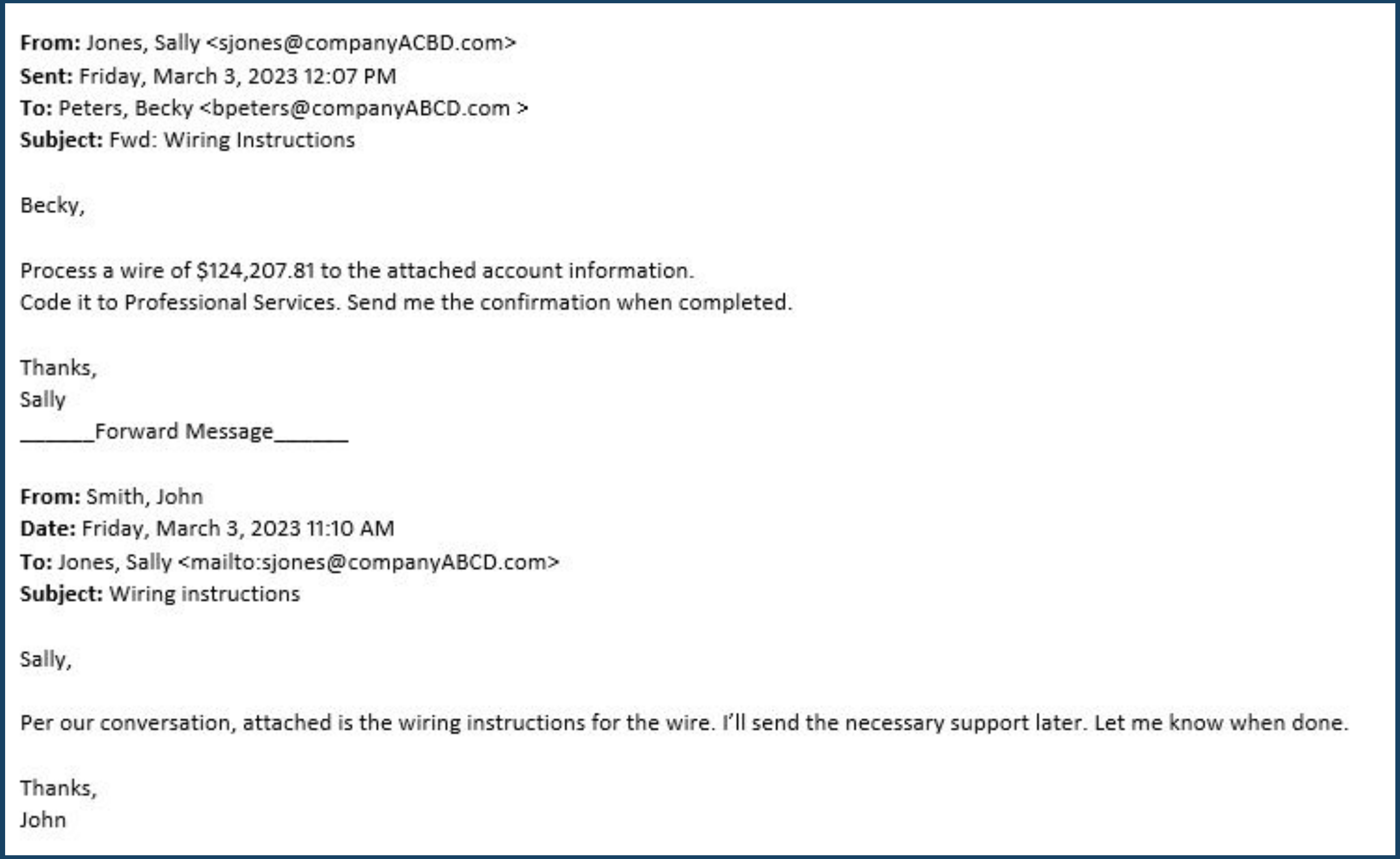
- It's highly scalable; multiple companies attacked at once.
- Companies are not prepared; you follow similar procedures.
- Authorized users make and authorize payments. Payments look normal to your bank.
- It's not quickly identified, and it's hard to recover funds – especially if sent by wire.
- Contact information, company organization structures, and sometimes payment instructions can often be found on company websites.
- Beneficiary name may not change with payment instructions.
- Routing number to Cash App, prepaid debit card bank (green dot, vanilla) is used heavily by the fraudsters

The biggest difference:

Fraudsters are willing and ready to interact with you. They anticipate you may question the request. They're prepared to respond to your follow-up emails and phone calls. Grammar of the fraudsters is not always a giveaway.

BEC Email Example

Spoofing Email Address – Business Masquerading



From: Jones, Sally <sjones@companyACBD.com>
Sent: Friday, March 3, 2023 12:07 PM
To: Peters, Becky <bpeters@companyABCD.com >
Subject: Fwd: Wiring Instructions

Becky,

Process a wire of $124,207.81 to the attached account information.
Code it to Professional Services. Send me the confirmation when completed.

Thanks,
Sally
______Forward Message______

From: Smith, John
Date: Friday, March 3, 2023 11:10 AM
To: Jones, Sally <mailto:sjones@companyABCD.com>
Subject: Wiring instructions

Sally,

Per our conversation, attached is the wiring instructions for the wire. I'll send the necessary support later. Let me know when done.

Thanks,
John

- Criminal's target is the Controller, Becky Peters.
- Mocks email from "CEO John Smith" to "CFO Sally Jones."
- Criminal creates a fake domain that is very close to the actual company domain in order to act as Sally.
- Criminal forwards fake email from "John" to Becky.
- Goal is to trick Becky into thinking it is a legitimate request.

Best Practices for Fighting BEC

- Alert and educate your executives and staff
- Alert and educate your internal business partners and vendors
- Authenticate payment requests out-of-band (verbally at a trusted phone number)
- Email requests for payment from executives should be prohibited
- Verbally verify any payment requests received by email at a trusted phone number
- Verbally verify any payment changes from an employee portal
- Implement dual control for money movement
- Be skeptical

Fraud Tips

- If it sounds to good to be true, it probably is.
- Trust but verify.
- Daily reconciliation.
- Keep computers up to date.
- Know your customer (does order or payment request or personal information request make sense)
- Use all available tools to protect a valuable asset - your money.
- Fraud continues to evolve… make fraud mitigation a part of your business culture.

Treasury Management

Krisha Fairchild – Manager, Treasury Management

FirstBank’s Treasury Management Team

- 50+ Employees, based out of Lakewood, CO
- Stringent verification methods
- Escalated money movement approvals
- How we can best assist you

Risk Mitigation

- Tokens
  - Physical and virtual tokens offered
  - Required for money movement approvals, optional at login and administrative changes
- IBM Trusteer Rapport
  - Free to download
  - Works alongside existing anti-virus software
- Alerts
  - Can be used as a tool for increased visibility into your account activity

Positive Pay

Positive Pay matches the account number, check number, and dollar amount of each check presented for payment against a list of checks previously authorized and issued by the company.

Good Candidates

- Issue a high volume of checks
- Have experienced check fraud
- Use accounting software
- Use a facsimile signature

ACH Block & Filter

ACH Block & Filter provides an essential added layer of security towards safeguarding your assets by automatically blocking or filtering out unauthorized ACH transactions.

How it works:

ACH filtering software in Internet Cash Management (ICM) will compare ACH transactions to your authorized list. When ACH transactions not on the list are presented, they are considered exceptions. Exceptions prompt a notification, which will give you the option to pay or return the exception in ICM.

Good Candidates

- Use ACH services
- Have experienced ACH fraud

Internal Controls

- Dual Custody/Restricted Admin
- Dual Processing
- Permissions
- ICM Administrator

Best Practices

- Know your employees
- Use a dedicated computer for ICM
- Monitor account activity
- Protect your login information
- Keep antivirus software, browsers, and operating systems updated

Q&A Panel

- Brenden Smith – Chief Information Security Officer at FirstBank
- Brad Champion – Director of Fraud Operations and Investigations at FirstBank
- Regan Coe – Treasury Management Development Supervisor
- Hilary Wells - Certified Information Privacy Professional and Partner at Lewis Roca