UNDERSTANDING CYBER SECURITY, FOR FINANCE PROFESSIONALS

John Thomas

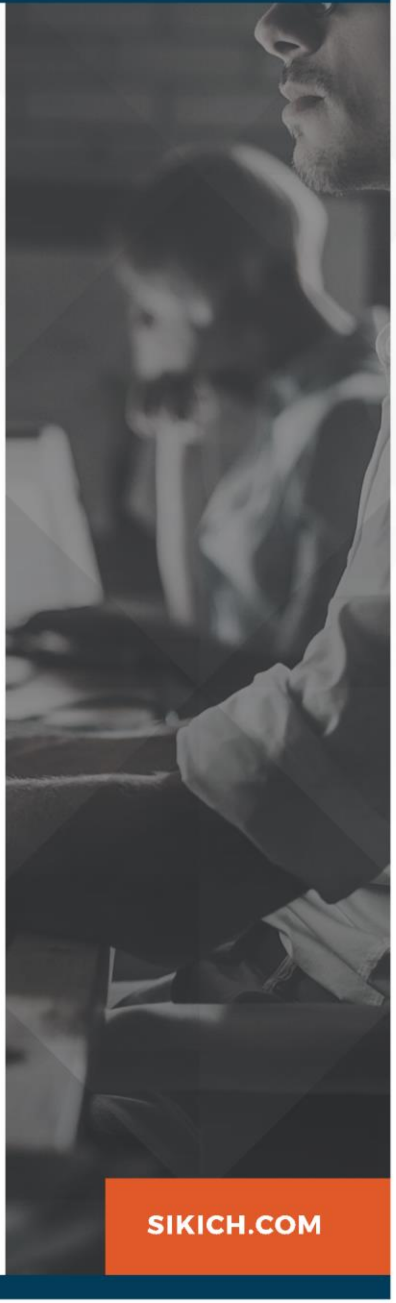
May 2019

SIKICH®

SIKICH.COM

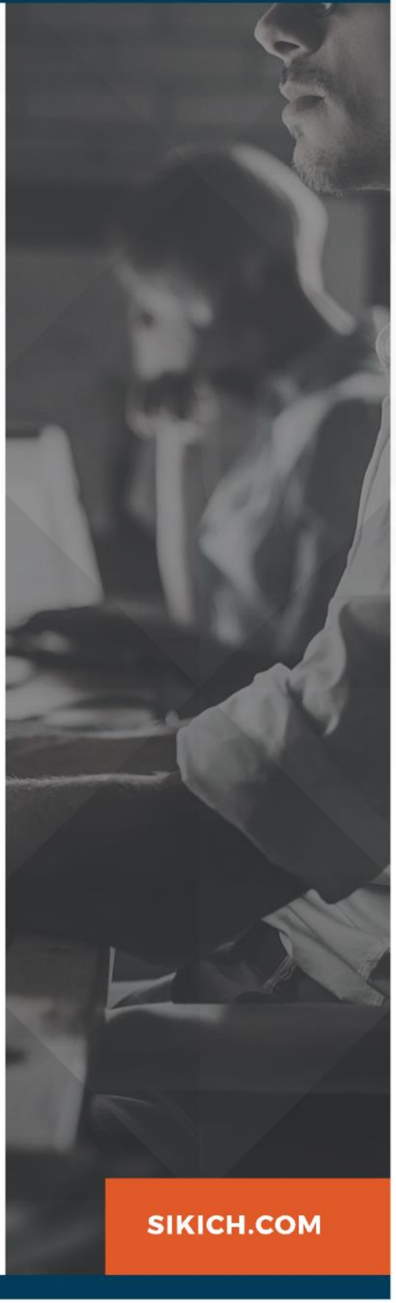
AGENDA

- Hackers and Breaches
- Monetizing Breaches
- Incident Response and Forensics
- Password Considerations
- Indicators of Infosec Program Maturity



AGENDA

- **HACKERS AND BREACHES**
- Monetizing Breaches
- Incident Response and Forensics
- Password Considerations
- Indicators of Infosec Program Maturity

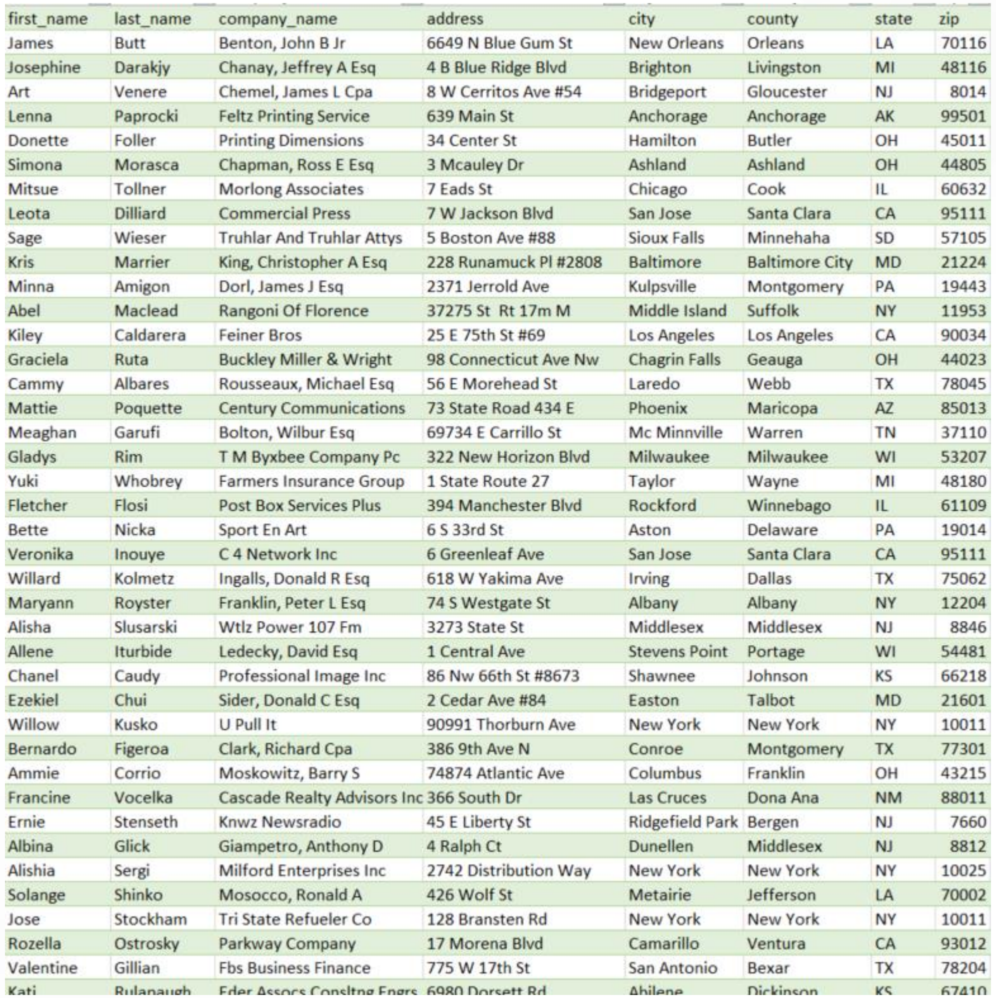


BREACHES - PAST

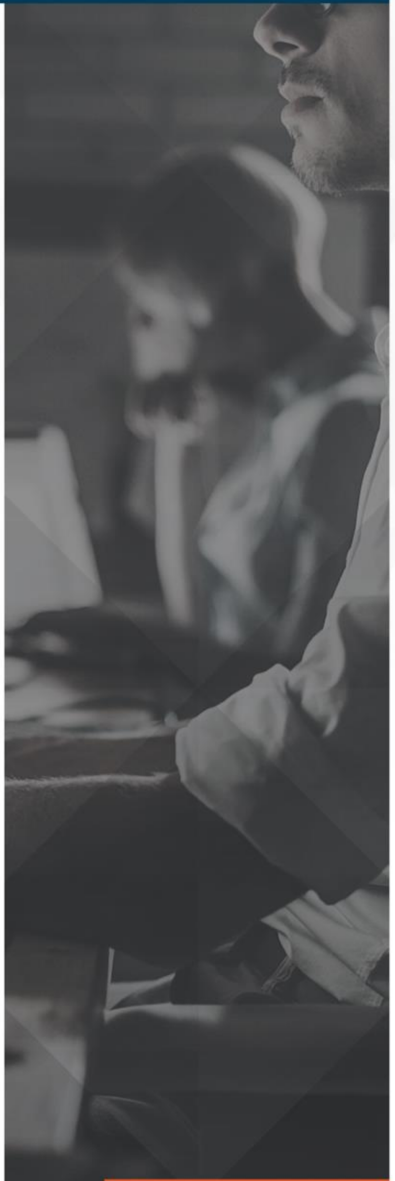
- Used to mainly target credit cards
  - TJ Maxx
  - Heartland Payment Systems
  - Ticketmaster
  - Target
  - Home Depot

BREACHES - TODAY

- Wider range of targets/data
  - Equifax
  - City of Atlanta
  - Sony
  - Ashley Madison
  - National Bank of Blacksburg

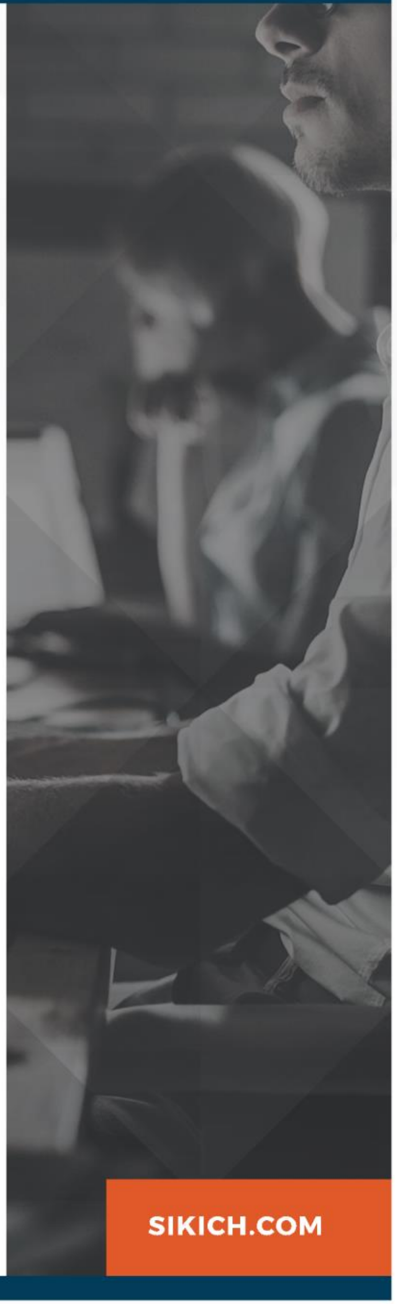


first_name	last_name	company_name	address	city	county	state	zip
James	Butt	Benton, John B Jr	6649 N Blue Gum St	New Orleans	Orleans	LA	70116
Josephine	Darakjy	Chanay, Jeffrey A Esq	4 B Blue Ridge Blvd	Brighton	Livingston	MI	48116
Art	Venere	Chemel, James L Cpa	8 W Cerritos Ave #54	Bridgeport	Gloucester	NJ	8014
Lenna	Paprocki	Feltz Printing Service	639 Main St	Anchorage	Anchorage	AK	99501
Donette	Foller	Printing Dimensions	34 Center St	Hamilton	Butler	OH	45011
Simona	Morasca	Chapman, Ross E Esq	3 Mcauley Dr	Ashland	Ashland	OH	44805
Mitsue	Tollner	Morlong Associates	7 Eads St	Chicago	Cook	IL	60632
Leota	Dilliard	Commercial Press	7 W Jackson Blvd	San Jose	Santa Clara	CA	95111
Sage	Wieser	Truhlar And Truhlar Attys	5 Boston Ave #88	Sioux Falls	Minnehaha	SD	57105
Kris	Marrier	King, Christopher A Esq	228 Runamuck Pl #2808	Baltimore	Baltimore City	MD	21224
Minna	Amigon	Dorl, James J Esq	2371 Jerrold Ave	Kulpsville	Montgomery	PA	19443
Abel	Maclead	Rangoni Of Florence	37275 St Rt 17m M	Middle Island	Suffolk	NY	11953
Kiley	Caldarera	Feiner Bros	25 E 75th St #69	Los Angeles	Los Angeles	CA	90034
Graciela	Ruta	Buckley Miller & Wright	98 Connecticut Ave Nw	Chagrin Falls	Geauga	OH	44023
Cammy	Albares	Rousseaux, Michael Esq	56 E Morehead St	Laredo	Webb	TX	78045
Mattie	Poquette	Century Communications	73 State Road 434 E	Phoenix	Maricopa	AZ	85013
Meaghan	Garufi	Bolton, Wilbur Esq	69734 E Carrillo St	Mc Minnville	Warren	TN	37110
Gladys	Rim	T M Byxbee Company Pc	322 New Horizon Blvd	Milwaukee	Milwaukee	WI	53207
Yuki	Whobrey	Farmers Insurance Group	1 State Route 27	Taylor	Wayne	MI	48180
Fletcher	Flosi	Post Box Services Plus	394 Manchester Blvd	Rockford	Winnebago	IL	61109
Bette	Nicka	Sport En Art	6 S 33rd St	Aston	Delaware	PA	19014
Veronika	Inouye	C 4 Network Inc	6 Greenleaf Ave	San Jose	Santa Clara	CA	95111
Willard	Kolmetz	Ingalls, Donald R Esq	618 W Yakima Ave	Irving	Dallas	TX	75062
Maryann	Royster	Franklin, Peter L Esq	74 S Westgate St	Albany	Albany	NY	12204
Alisha	Slusarski	Wtlz Power 107 Fm	3273 State St	Middlesex	Middlesex	NJ	8846
Allene	Iturbide	Ledecky, David Esq	1 Central Ave	Stevens Point	Portage	WI	54481
Chanel	Caudy	Professional Image Inc	86 Nw 66th St #8673	Shawnee	Johnson	KS	66218
Ezekiel	Chui	Sider, Donald C Esq	2 Cedar Ave #84	Easton	Talbot	MD	21601
Willow	Kusko	U Pull It	90991 Thorburn Ave	New York	New York	NY	10011
Bernardo	Figeroa	Clark, Richard Cpa	386 9th Ave N	Conroe	Montgomery	TX	77301
Ammie	Corrio	Moskowitz, Barry S	74874 Atlantic Ave	Columbus	Franklin	OH	43215
Francine	Vocelka	Cascade Realty Advisors Inc	366 South Dr	Las Cruces	Dona Ana	NM	88011
Ernie	Stenseth	Knwz Newsradio	45 E Liberty St	Ridgefield Park	Bergen	NJ	7660
Albina	Glick	Giampetro, Anthony D	4 Ralph Ct	Dunellen	Middlesex	NJ	8812
Alishia	Sergi	Milford Enterprises Inc	2742 Distribution Way	New York	New York	NY	10025
Solange	Shinko	Mosocco, Ronald A	426 Wolf St	Metairie	Jefferson	LA	70002
Jose	Stockham	Tri State Refueler Co	128 Bransten Rd	New York	New York	NY	10011
Rozella	Ostrosky	Parkway Company	17 Morena Blvd	Camarillo	Ventura	CA	93012
Valentine	Gillian	Fbs Business Finance	775 W 17th St	San Antonio	Bexar	TX	78204
Kati	Rulapaugh	Eder Assocs Consltng Engrs	6980 Dorsett Rd	Abilene	Dickinson	KS	67410



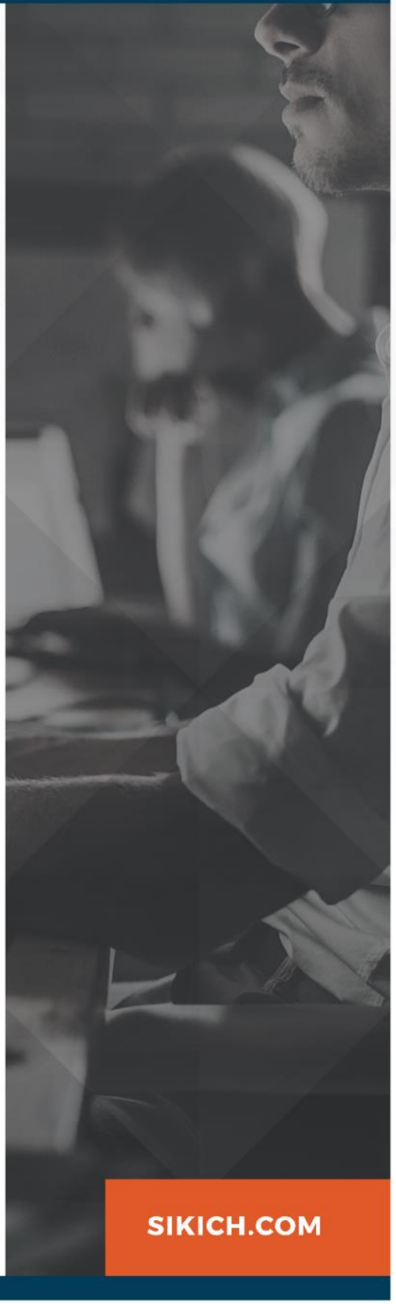
TARGETS OF CHANCE

- Attacker casts a wide net
- May know how to exploit one website vulnerability in off-the-shelf website software
  - Sets up a scan to try that exploit against every website
- Generalized phishing attacks
  - Thousands or millions of recipients
- Brute-force password guessing
- Self-propagating viruses
  - Some have built-in logic to test for something of interest – banking credentials or card payment applications
  - Otherwise spread



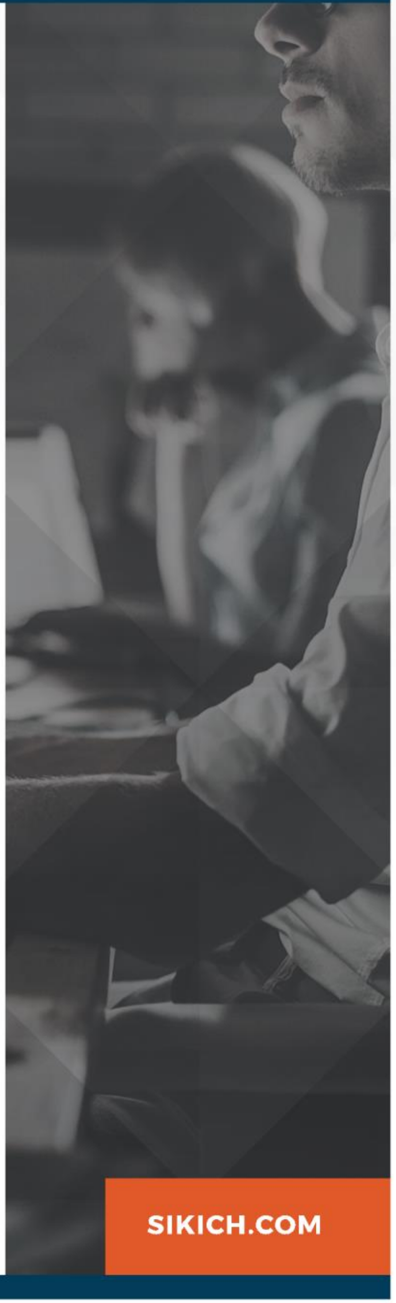
TARGETS OF CHOICE

- Attacker has selected an organization as a target
- Automated and manual inspection of website for weaknesses
- **Spearphishing**
- Targeted password guessing
- Custom-built malware



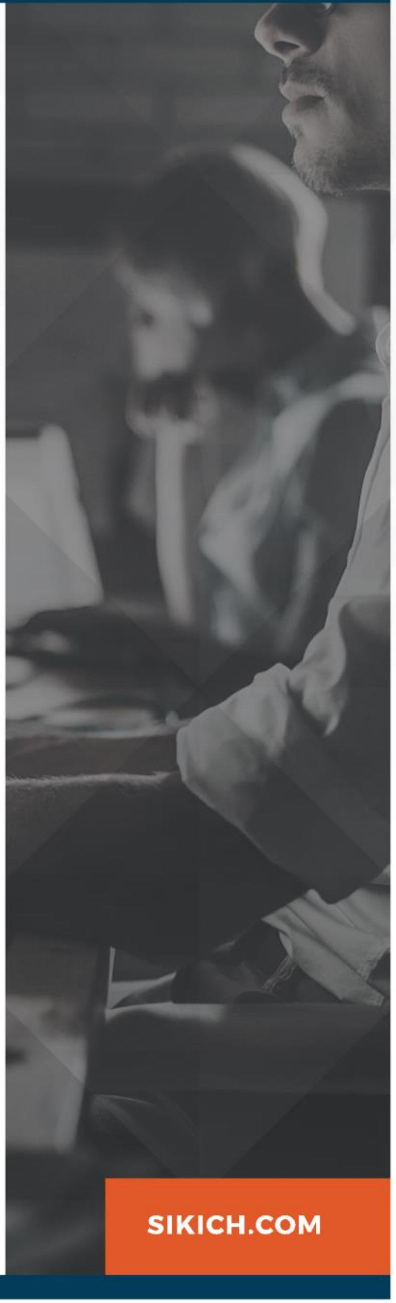
COMMUNITY COLLEGES INCREASINGLY ARE TARGETS

- Lowest hanging fruit for attacks
  - Personal Information
  - Student Loans
  - SS Numbers used as identifiers
  - Cybersecurity “not a priority”
- Increasingly connected
  - Remote and mobile student body
  - Technology critical for education, operations, and service
  - Increasing use of cloud services
- Attackers have perfected multiple channels for monetizing community college breaches



AGENDA

- Hackers and Breaches
- **MONETIZING BREACHES**
- Incident Response and Forensics
- Password Considerations
- Indicators of Infosec Program Maturity

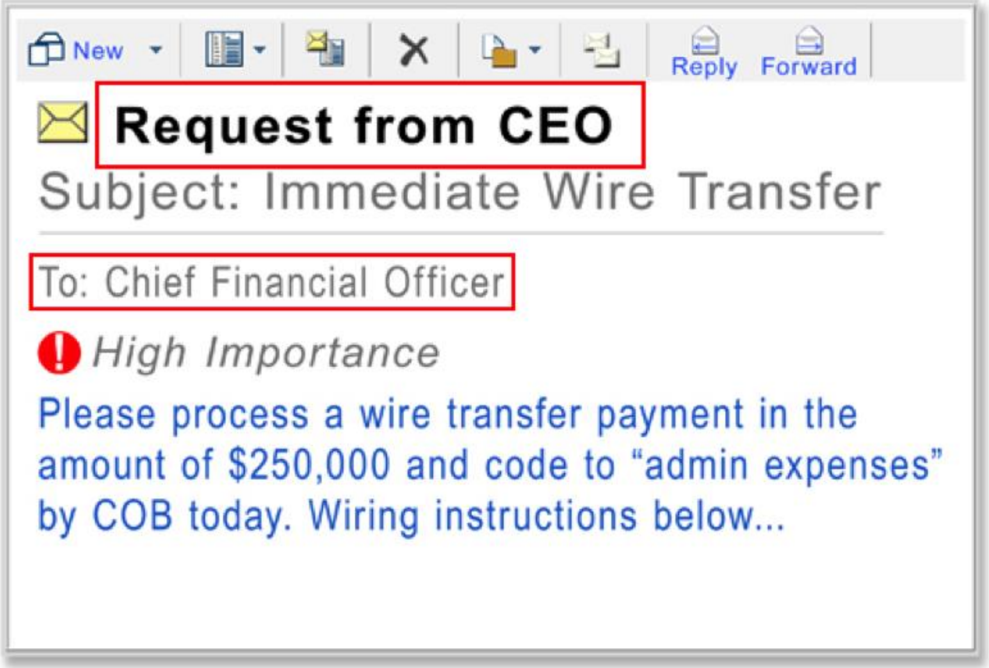


STUDENT LOAN FRAUD

- Thieves apply for loans using stolen personal information
- Federal funding goes to the school for tuition and fees, balance is remanded to the "student"
- Victim is left on the hook for the debt

ELECTRONIC PAYMENT FRAUD

- Sometimes called “email account takeover” since they are so intertwined
- ACH and wire fraud most common
- “Business” bank accounts don’t include the same consumer protections as personal accounts
- Victims usually take the loss



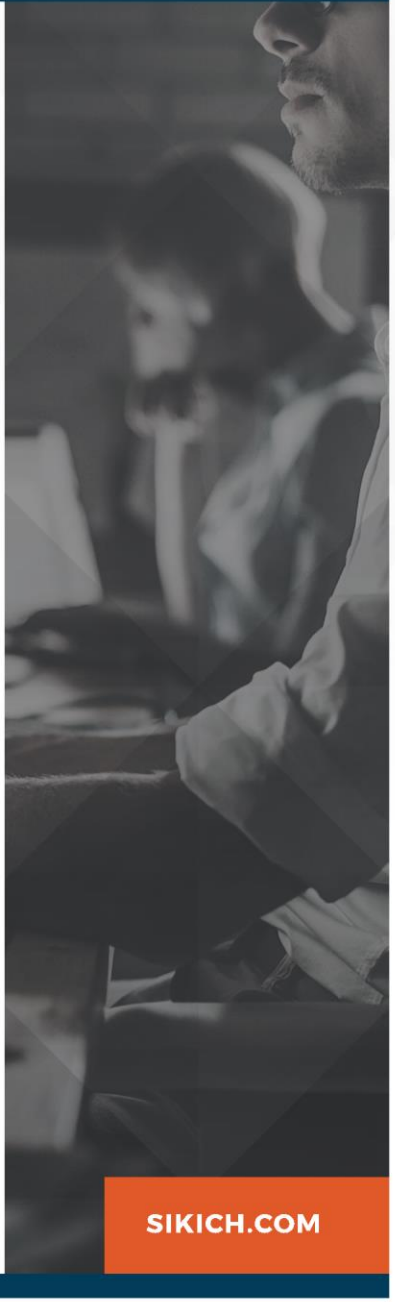
Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

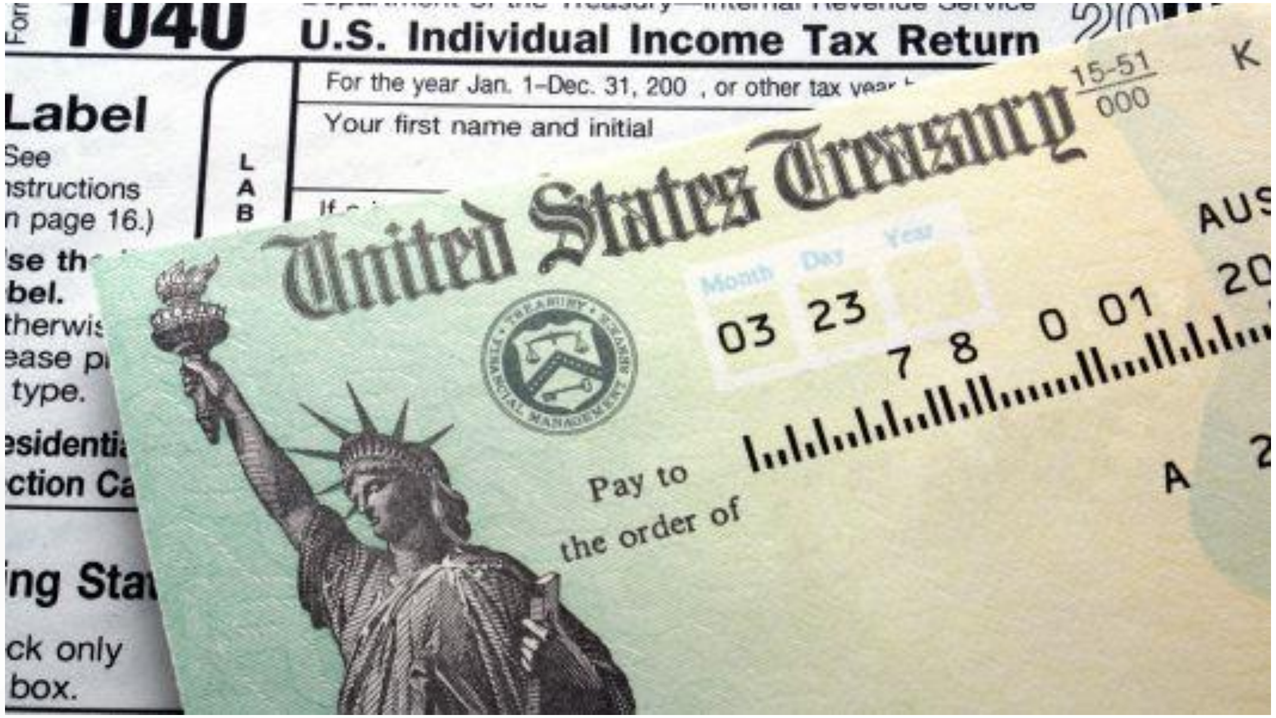
High Importance

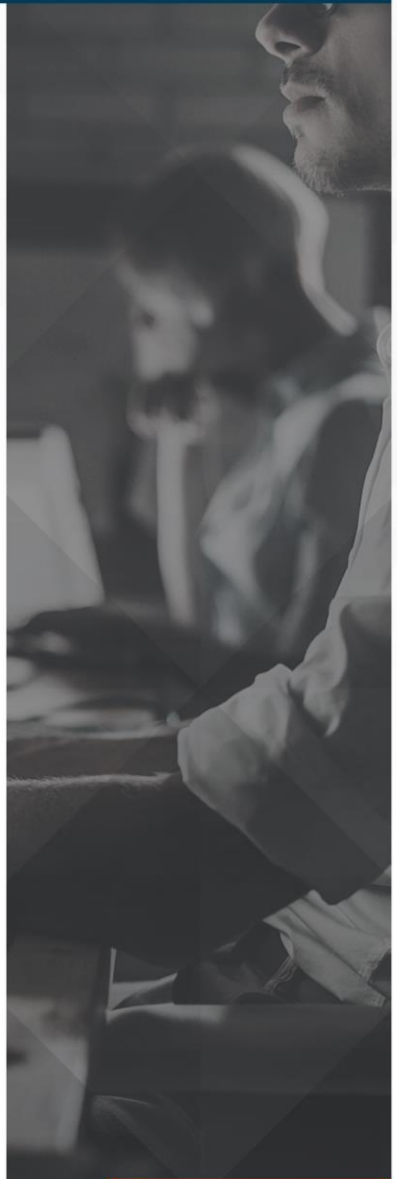
Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...



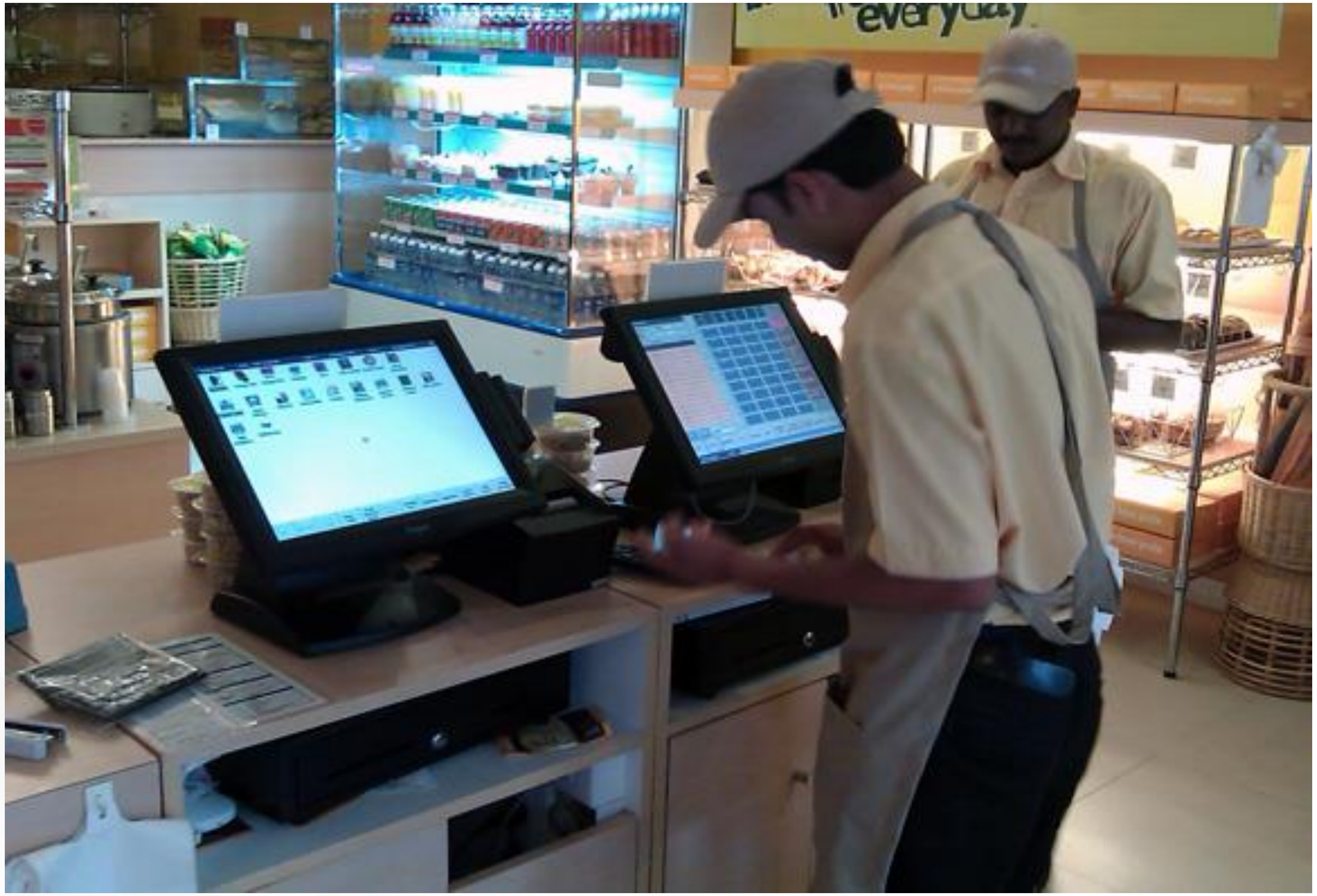
TAX RETURN FRAUD

- Relatively easy and low-risk form of identity theft
- Requires knowledge of name, DOB and SSN

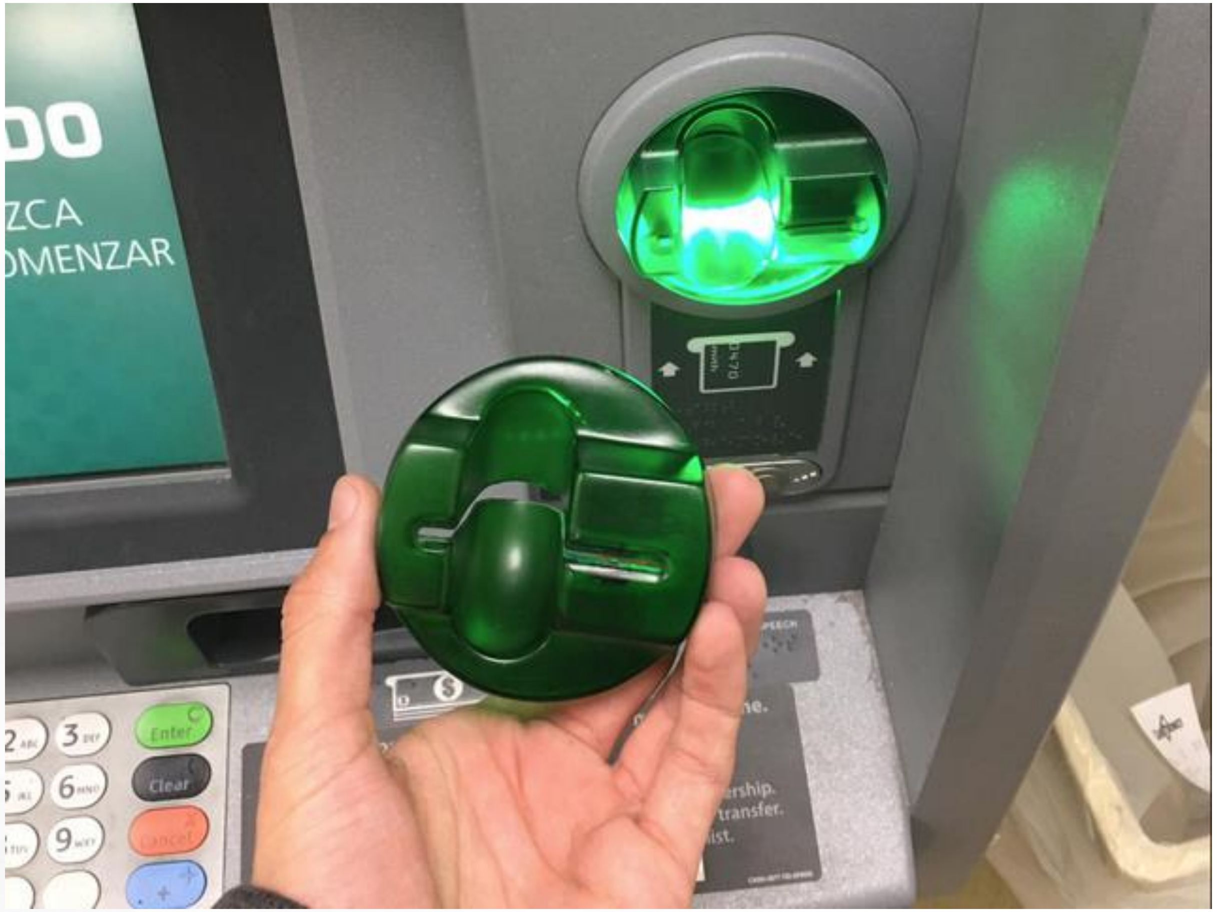

1040
U.S. Individual Income Tax Return
For the year Jan. 1–Dec. 31, 200 , or other tax year
Your first name and initial
Label
See instructions on page 16.)
United States Treasury
15-51
000
Month Day Year
03 23
7 8 0 01
Pay to the order of



CREDIT CARD FRAUD – INFECTED COMPUTERS



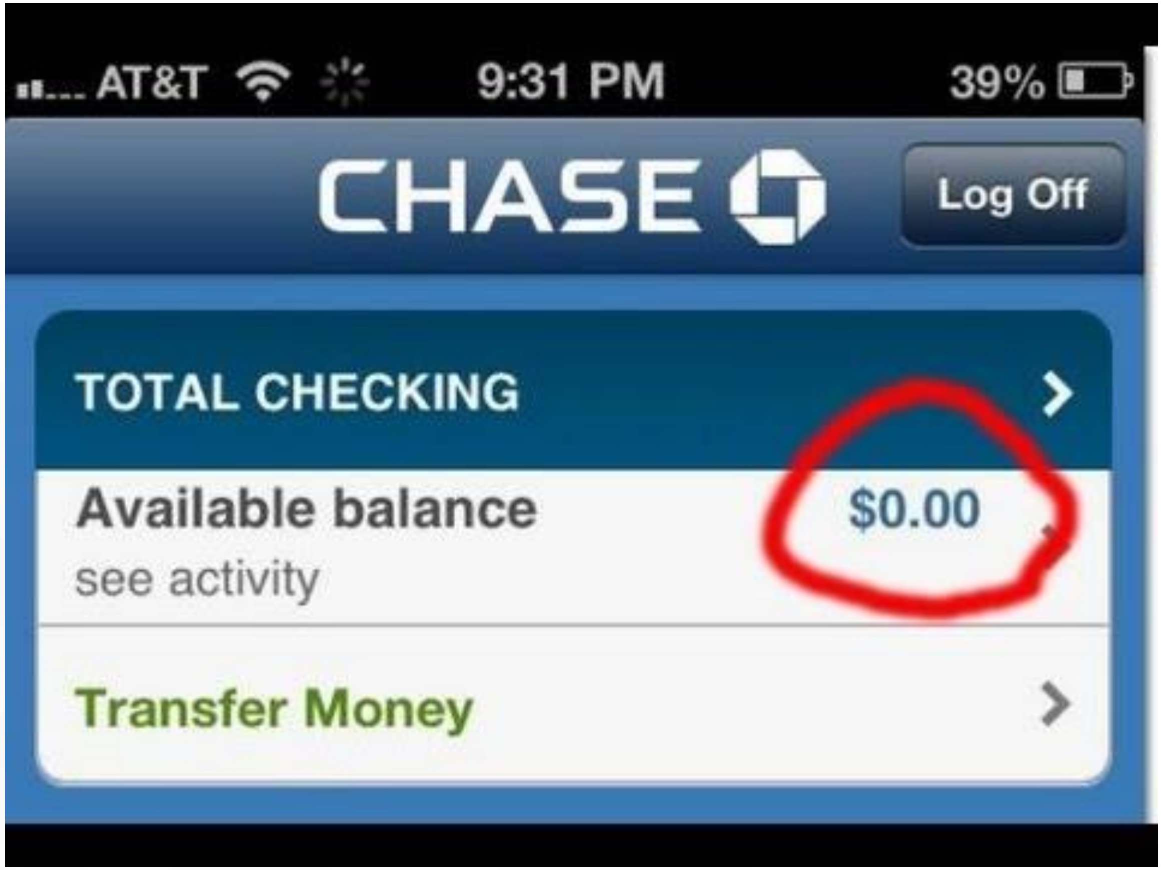
CREDIT CARD FRAUD – CARD SKIMMERS



DON'T CHIP-ENABLED CARDS STOP FRAUD?

- EMV-only cards make it harder to create a forged physical card
- Does not impact online/phone sales
- Does not prevent use of stolen cards
- Does not increase the security of networks or backend systems
- Why switch?
  - Otherwise your college can take the loss if someone pays with a forged card in hand

A BAD MONDAY MORNING

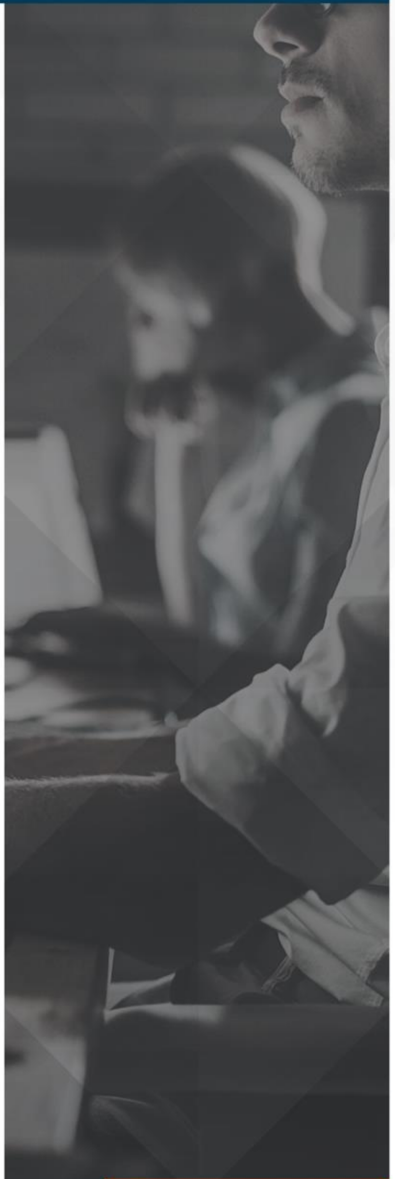


TOTAL CHECKING

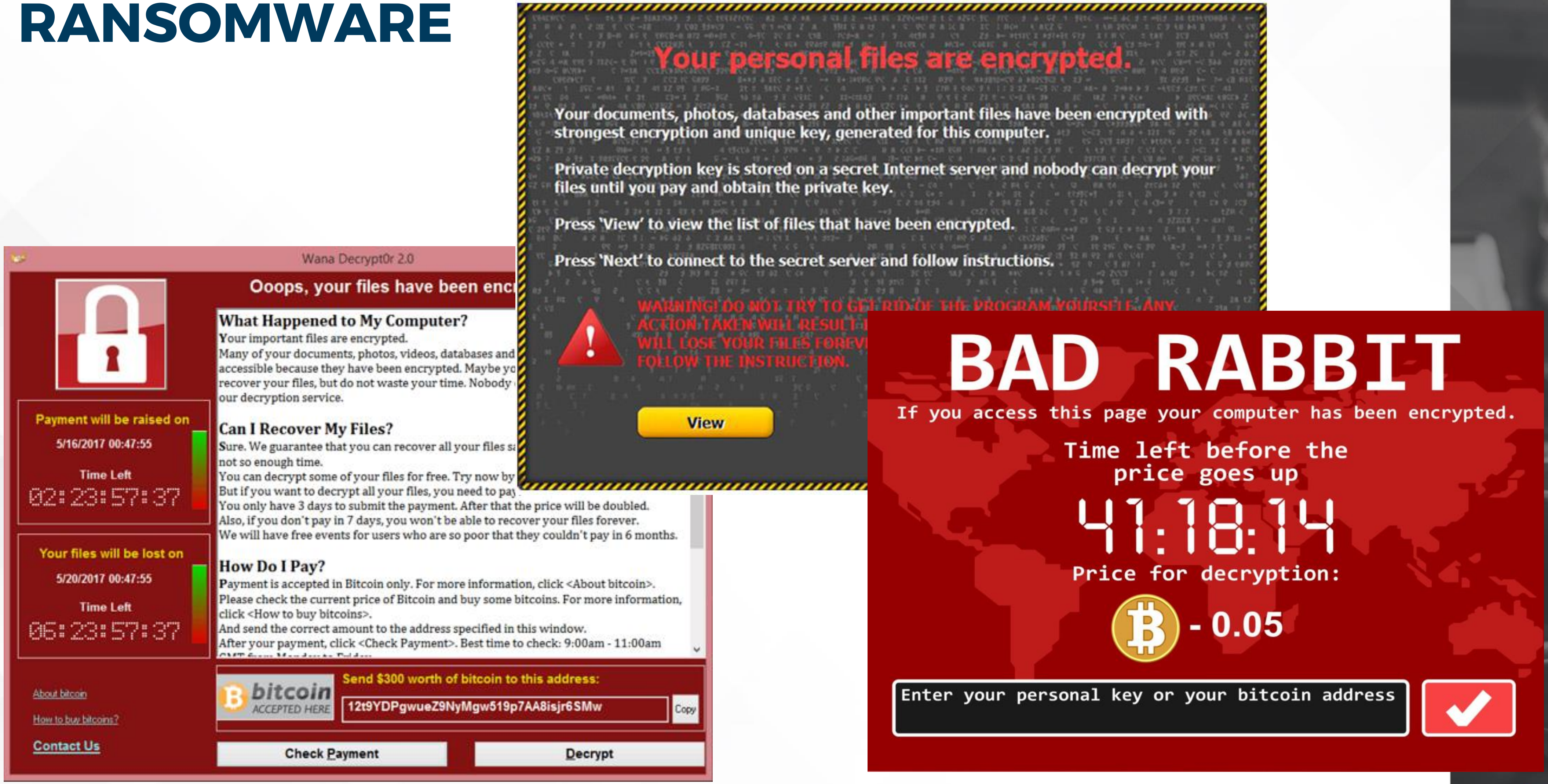
Available balance $0.00

see activity

Transfer Money



RANSOMWARE



Wana Decrypt0r 2.0

Ooops, your files have been enc

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and
accessible because they have been encrypted. Maybe yo
recover your files, but do not waste your time. Nobody
our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files sa
not so enough time.
You can decrypt some of your files for free. Try now by
But if you want to decrypt all your files, you need to pay
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY
ACTION TAKEN WILL RESULT I
WILL LOSE YOUR FILES FOREV
FOLLOW THE INSTRUCTION.

BAD RABBIT

If you access this page your computer has been encrypted.

Time left before the
price goes up

41:18:14

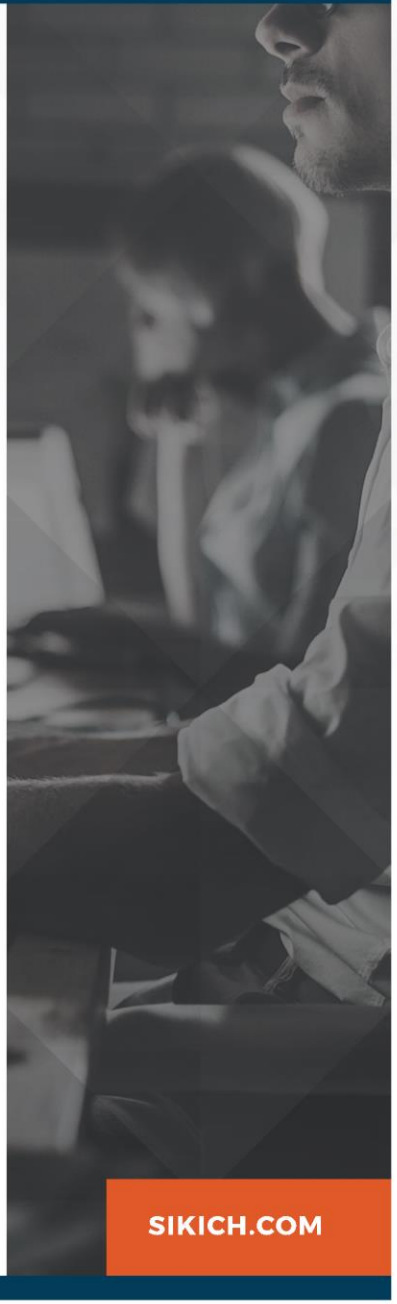
Price for decryption:

- 0.05

Enter your personal key or your bitcoin address

CYBER EXTORTION

- Harvest your data
- Demand Bitcoin payment or they will publicly disclose the breach or leak the data

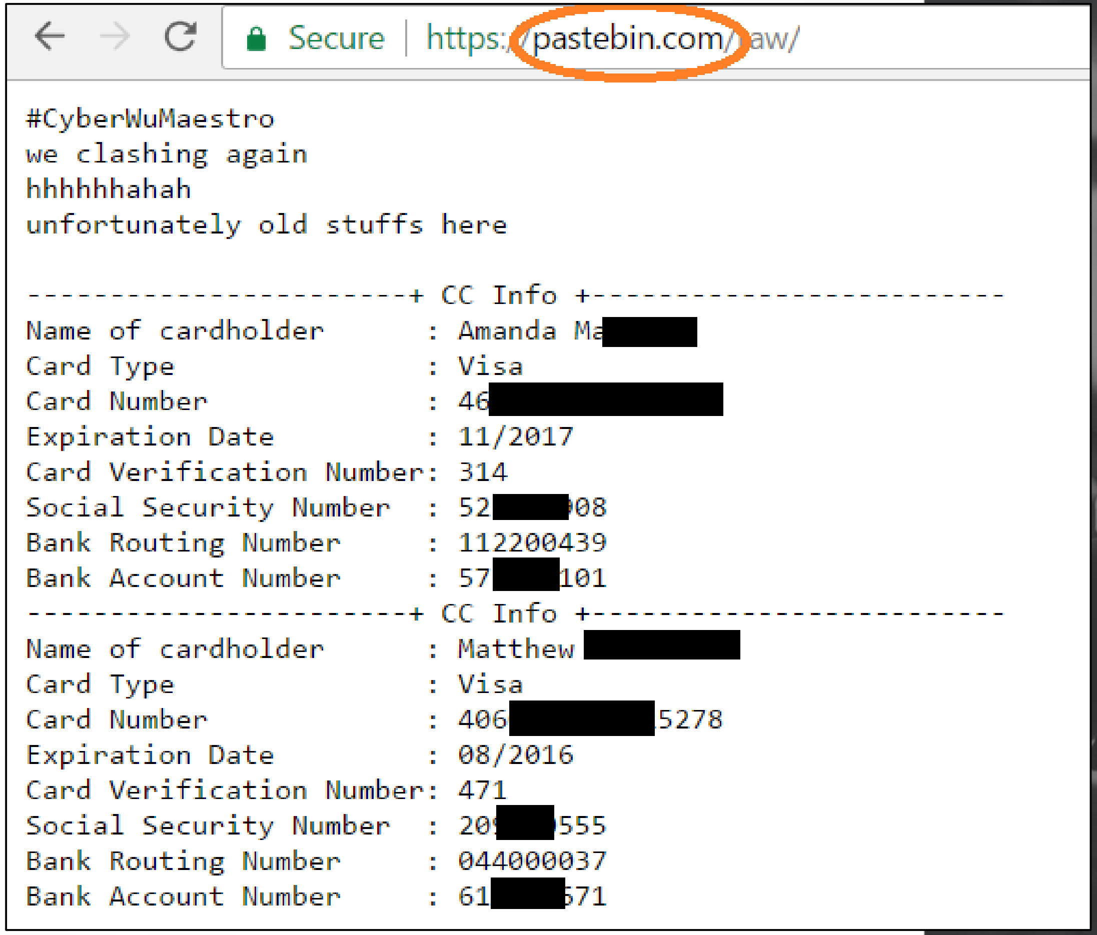


CRYPTOCURRENCY MINING

- Increasingly sophisticated to avoid getting flagged
  - Slow down the speed of CPU fans
  - Switching off mining software during a users' active hours
  - Artificially showing low computing power usage

SELLING DATA ON THE “DARK WEB”

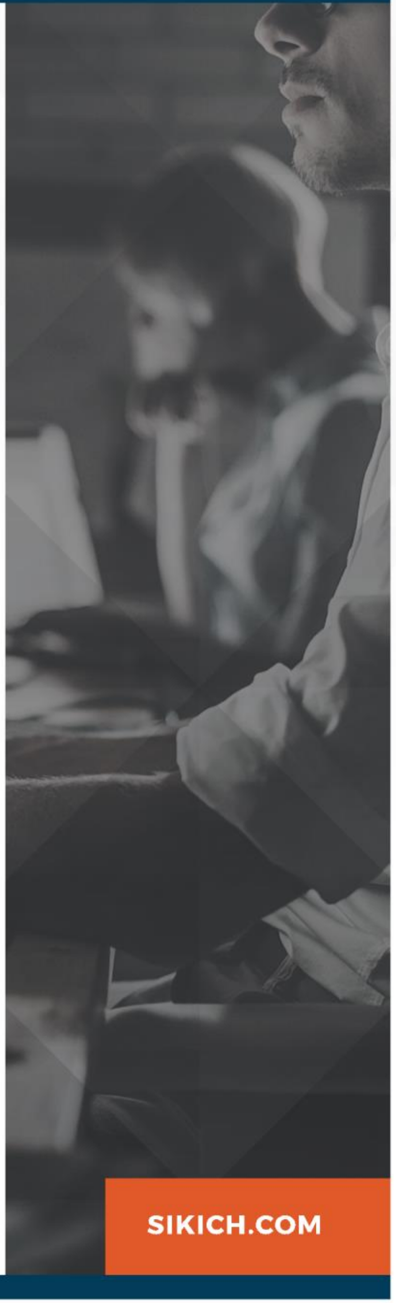
- Credentials to sell
  - Student, professor, etc. usernames and passwords
  - Personal accounts
  - School accounts



```
#CyberWuMaestro
we clashing again
hhhhhhahah
unfortunately old stuffs here

-----------------------+ CC Info +------------------------
Name of cardholder        : Amanda Ma[redacted]
Card Type                 : Visa
Card Number               : 46[redacted]
Expiration Date           : 11/2017
Card Verification Number: 314
Social Security Number   : 52[redacted]08
Bank Routing Number       : 112200439
Bank Account Number       : 57[redacted]101
-----------------------+ CC Info +------------------------
Name of cardholder        : Matthew [redacted]
Card Type                 : Visa
Card Number               : 406[redacted]5278
Expiration Date           : 08/2016
Card Verification Number: 471
Social Security Number   : 20[redacted]555
Bank Routing Number       : 044000037
Bank Account Number       : 61[redacted]71
```

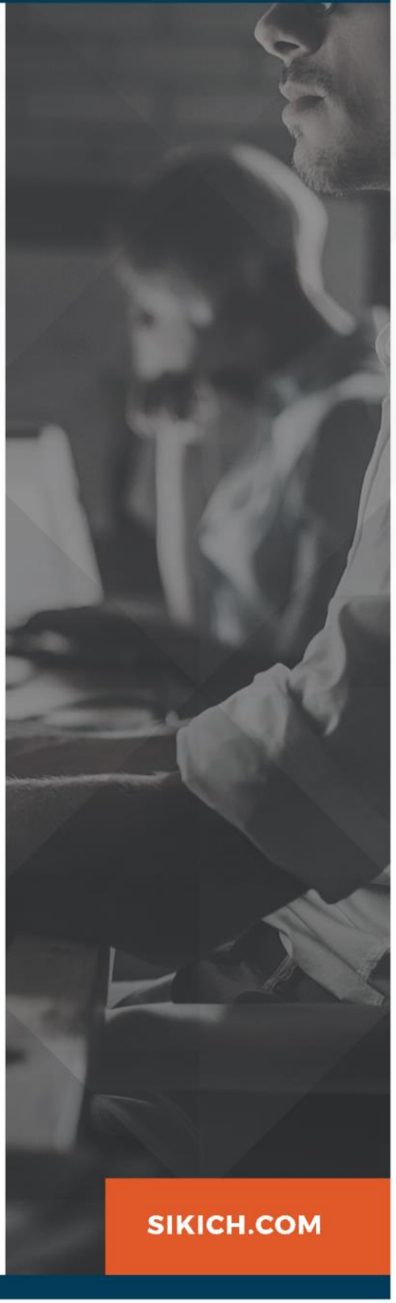
AGENDA

- Hackers and Breaches
- Monetizing Breaches
- **INCIDENT RESPONSE AND FORENSICS**
- Password Considerations
- Indicators of Infosec Program Maturity



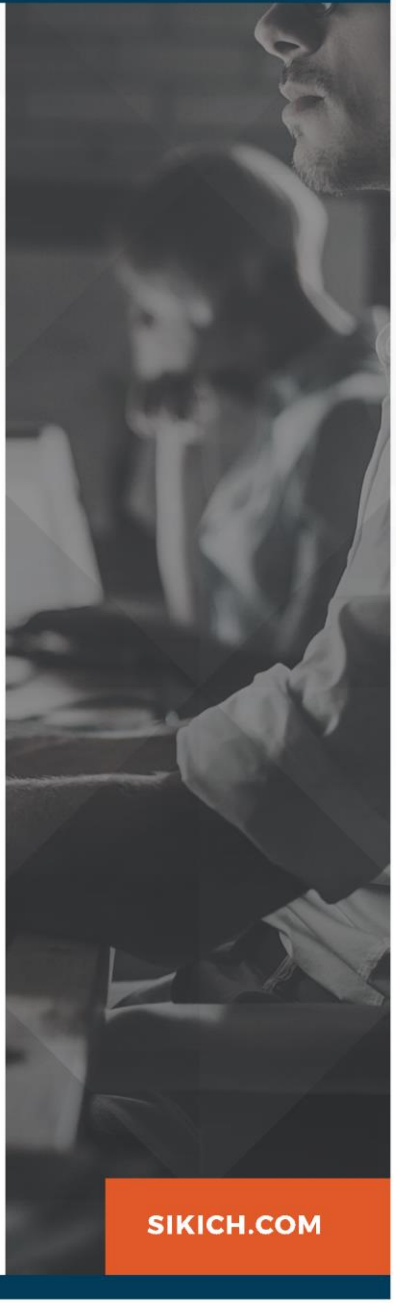
RECENT TRENDS FROM FORENSIC INVESTIGATIONS

- Drastic changes in attacks in the past year
  - Method
  - Willingness to persist
- Attackers fighting to hold ground even after detection
- The professional criminals are handpicking their victims
  - (No more just outrunning the bear)



WHAT HAPPENS WHEN A BREACH OCCURS

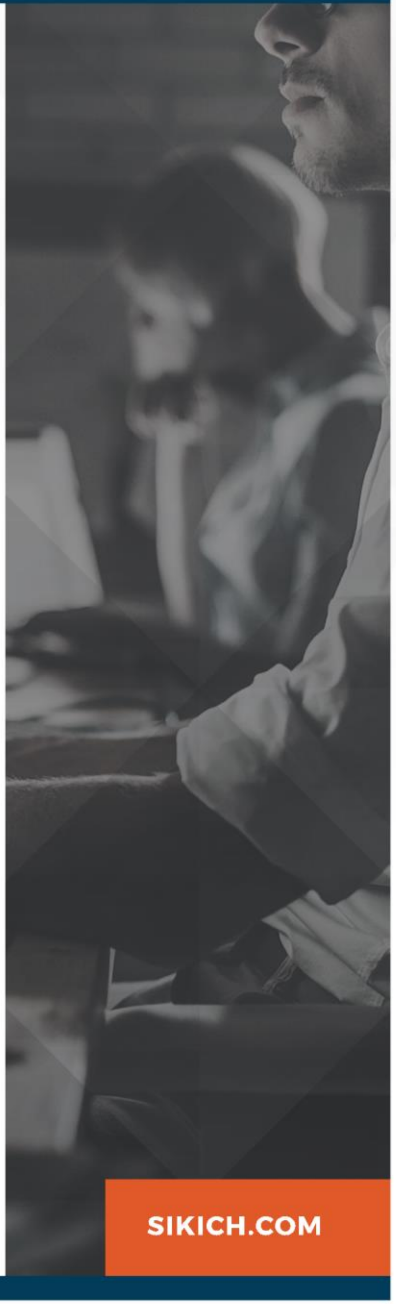
- Response activities may be driven by your bank or regulatory bodies
- Forensic investigations typically cost $20,000 and up
  - Collection and analysis of data
  - Attempt to determine how they got in and what they took
  - Seldom able to gather a complete record of the event
- Determine breach notification requirements
- Community college and media communications management



INCIDENT RESPONSE

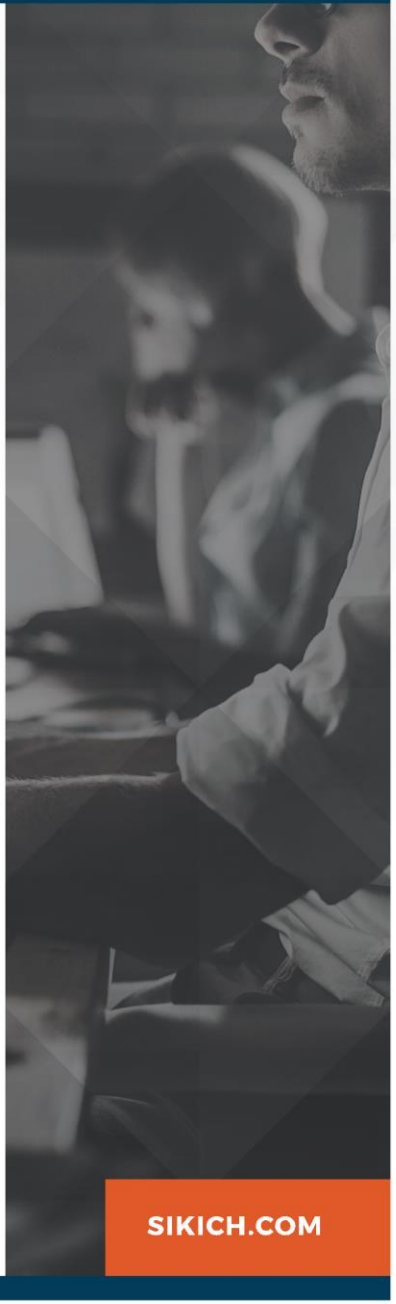
- Identification
  - Is this a real incident
- Containment
  - Stop the bleeding
- Eradication
  - Remove the cause
  - Create indicators of compromise
- Recovery
  - Best route back to a trusted environment

- All the time balance these activities against facilitating day to day processes and maintaining evidence



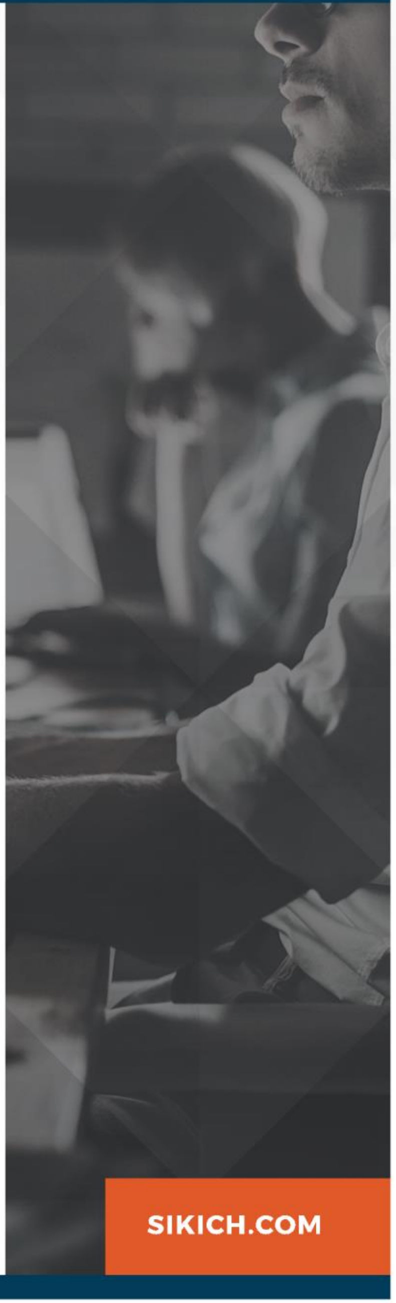
FORENSIC INVESTIGATION

- Formal review/inspection of the event
- Disk and memory imaging of impacted systems
- Collection of log files
- Offline analysis of images
  - Timeline analysis
  - File integrity analysis
- Often the “smoking gun” and the whole picture cannot be identified



AGENDA

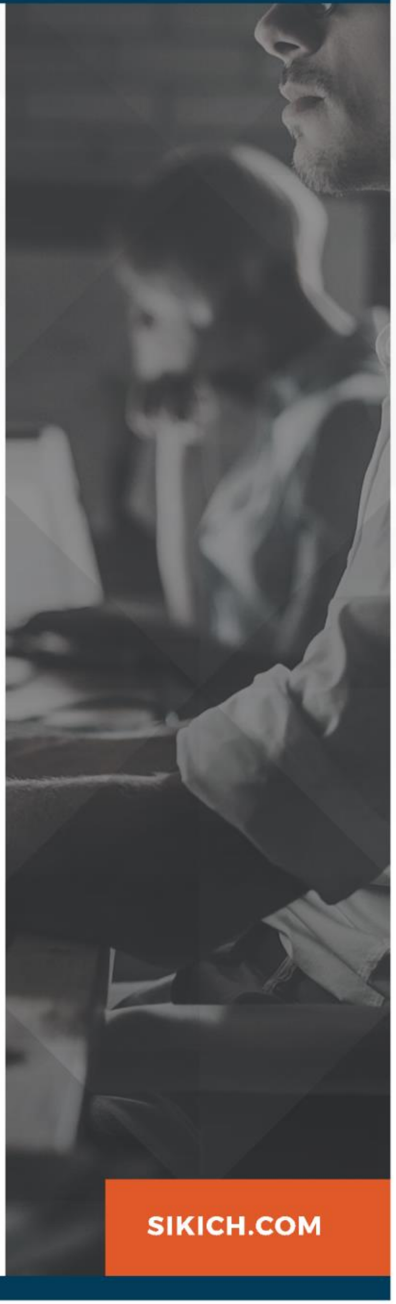
- Hackers and Breaches
- Monetizing Breaches
- Incident Response and Forensics
- **PASSWORD CONSIDERATIONS**
- Indicators of Infosec Program Maturity



JUST ONE PASSWORD

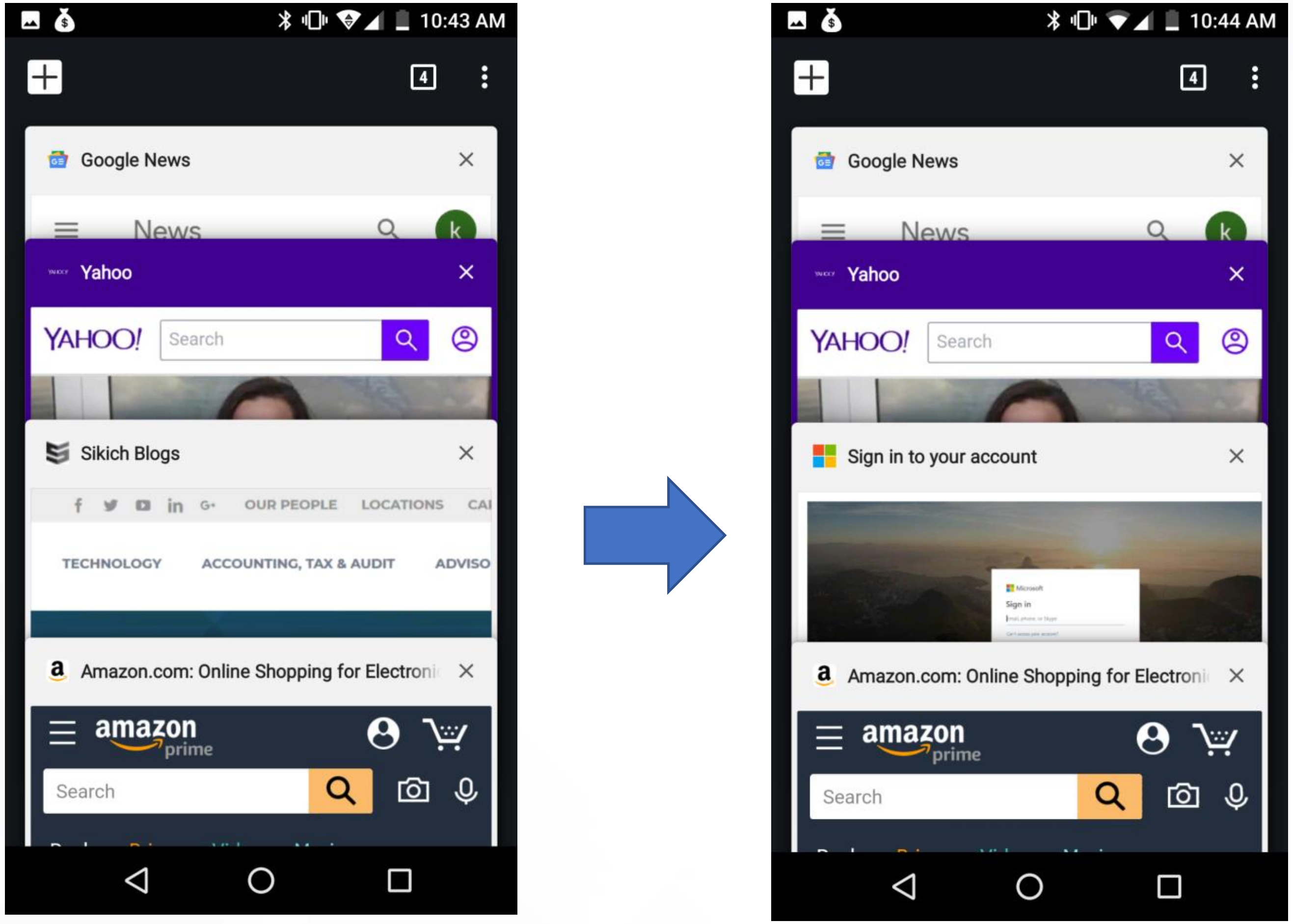
- From Outside
  - Email
  - Cloud file services
  - Registration, Payroll and Benefits sites

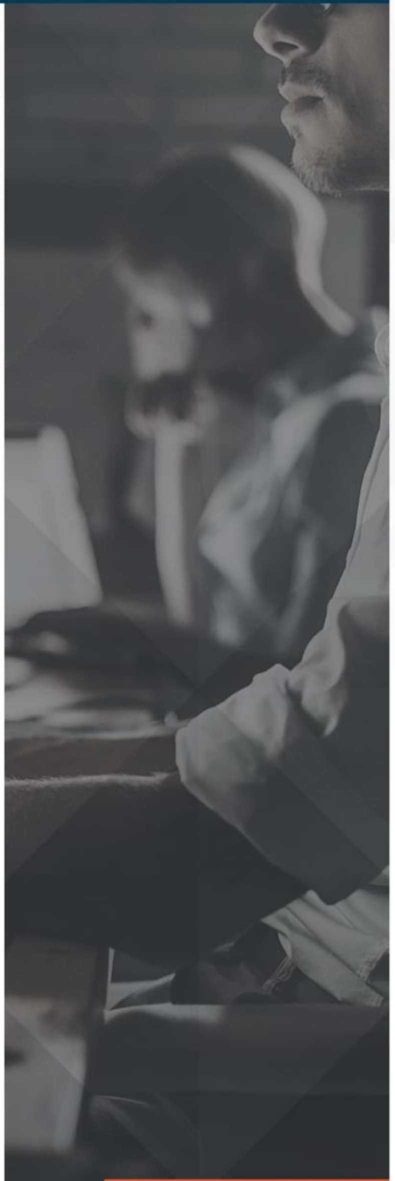
- From Inside
  - Query network for username list, who is admin
  - Unprotected/open network shares
  - Login to a workstation and run a keylogger



INCREASINGLY SOPHISTICATED PHISHING ATTACKS

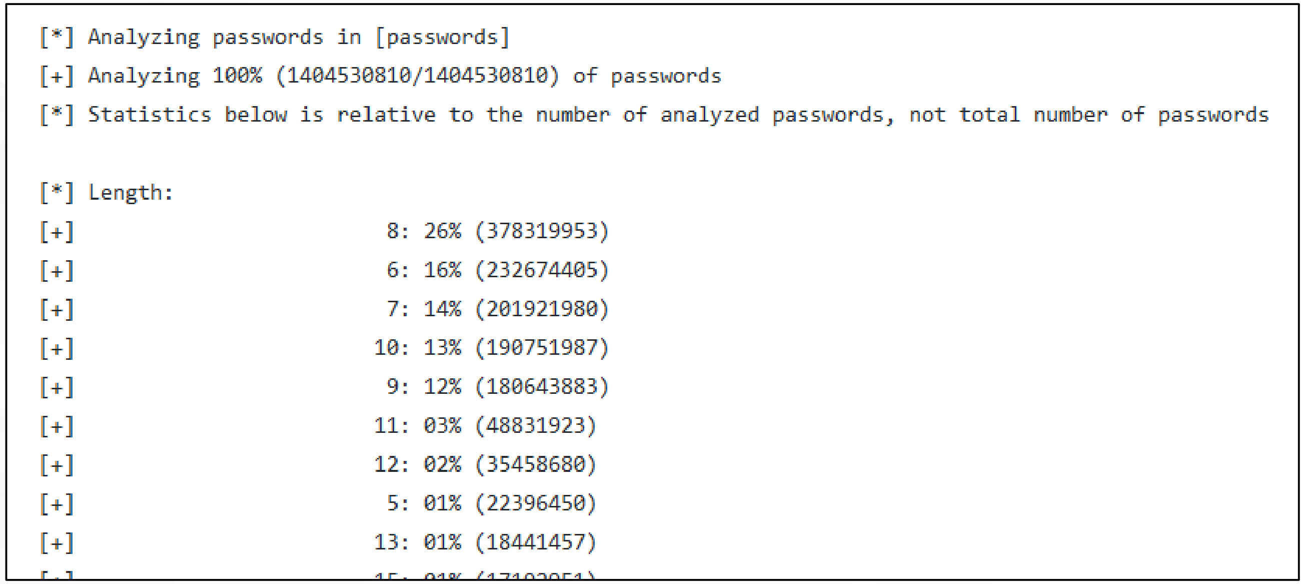
- Spearphishing
- Tab nabbing



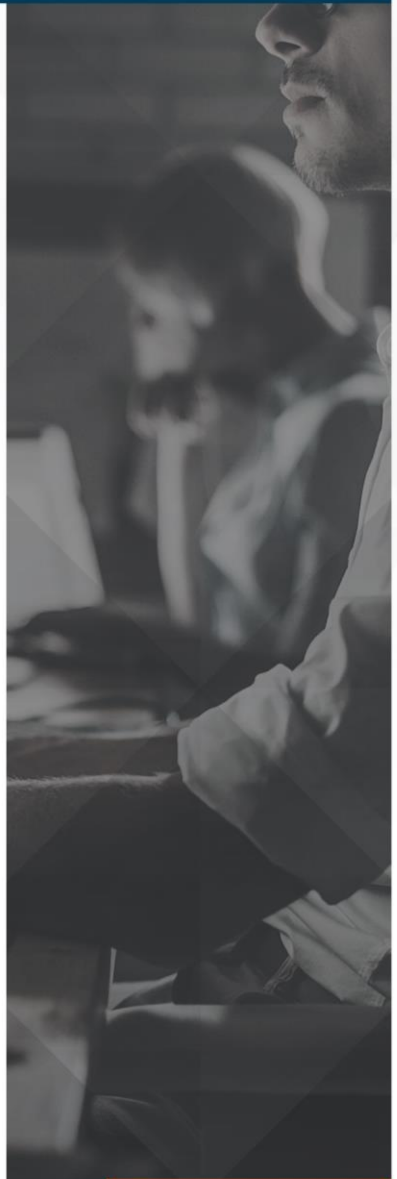


WEBSITE BREACH LISTS

- Many breaches result in theft of email/password pairings
- These lists are often leaked to the Internet
- Used in “credential stuffing” attacks

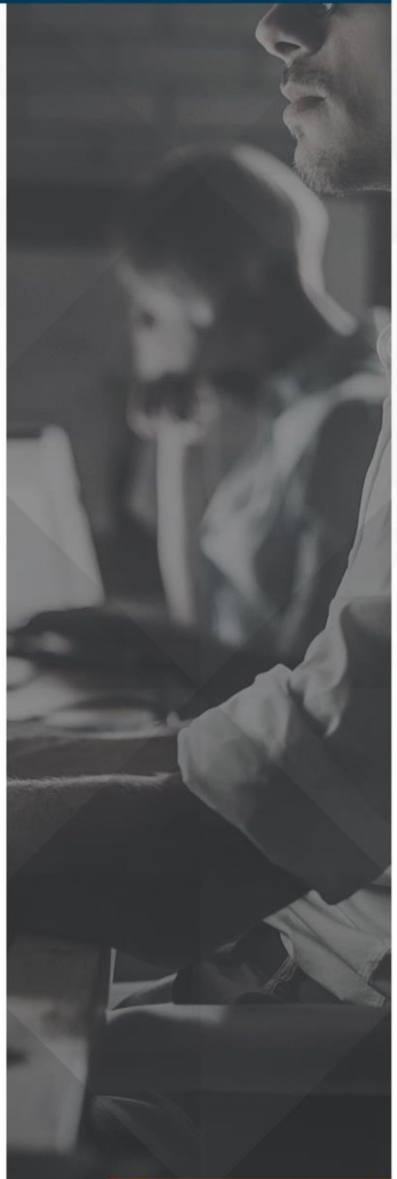


```
[*] Analyzing passwords in [passwords]
[+] Analyzing 100% (1404530810/1404530810) of passwords
[*] Statistics below is relative to the number of analyzed passwords, not total number of passwords

[*] Length:
[+]                         8: 26% (378319953)
[+]                         6: 16% (232674405)
[+]                         7: 14% (201921980)
[+]                        10: 13% (190751987)
[+]                         9: 12% (180643883)
[+]                        11: 03% (48831923)
[+]                        12: 02% (35458680)
[+]                         5: 01% (22396450)
[+]                        13: 01% (18441457)
[+]                        15: 01% (17102951)
```



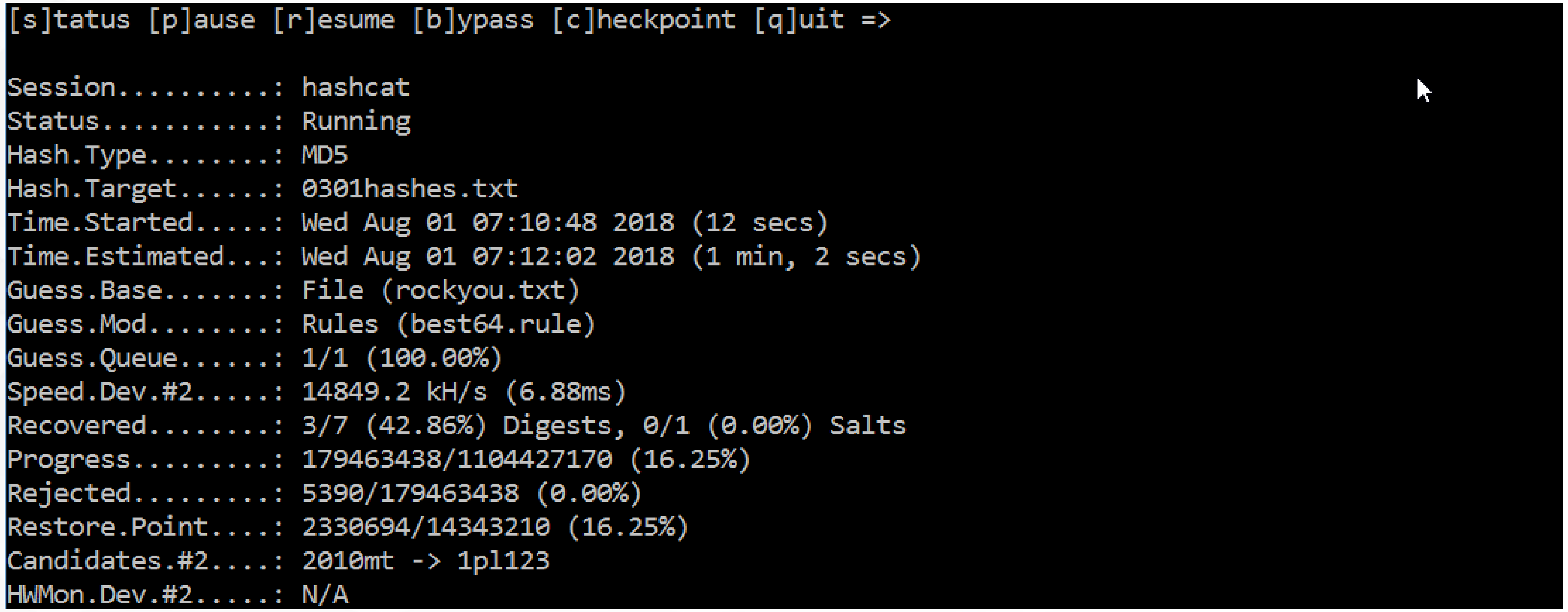
PASSWORD SPRAYING

- Guessing 500 passwords against one account → Lockout
- Guessing one password against 500 accounts → Often success
- Common password examples
    - Packers1
    - July2018
    - Summer18
    - Username as password
    - Welcome123

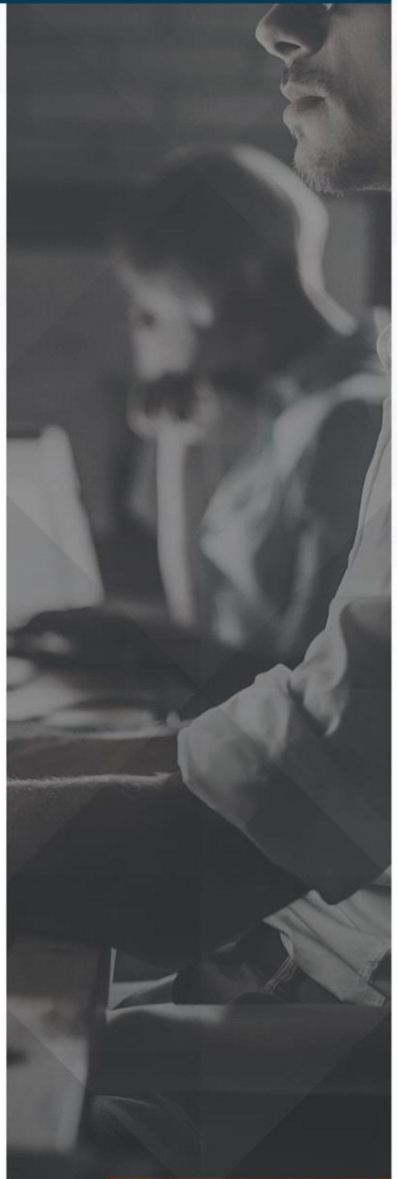


PASSWORD CRACKING

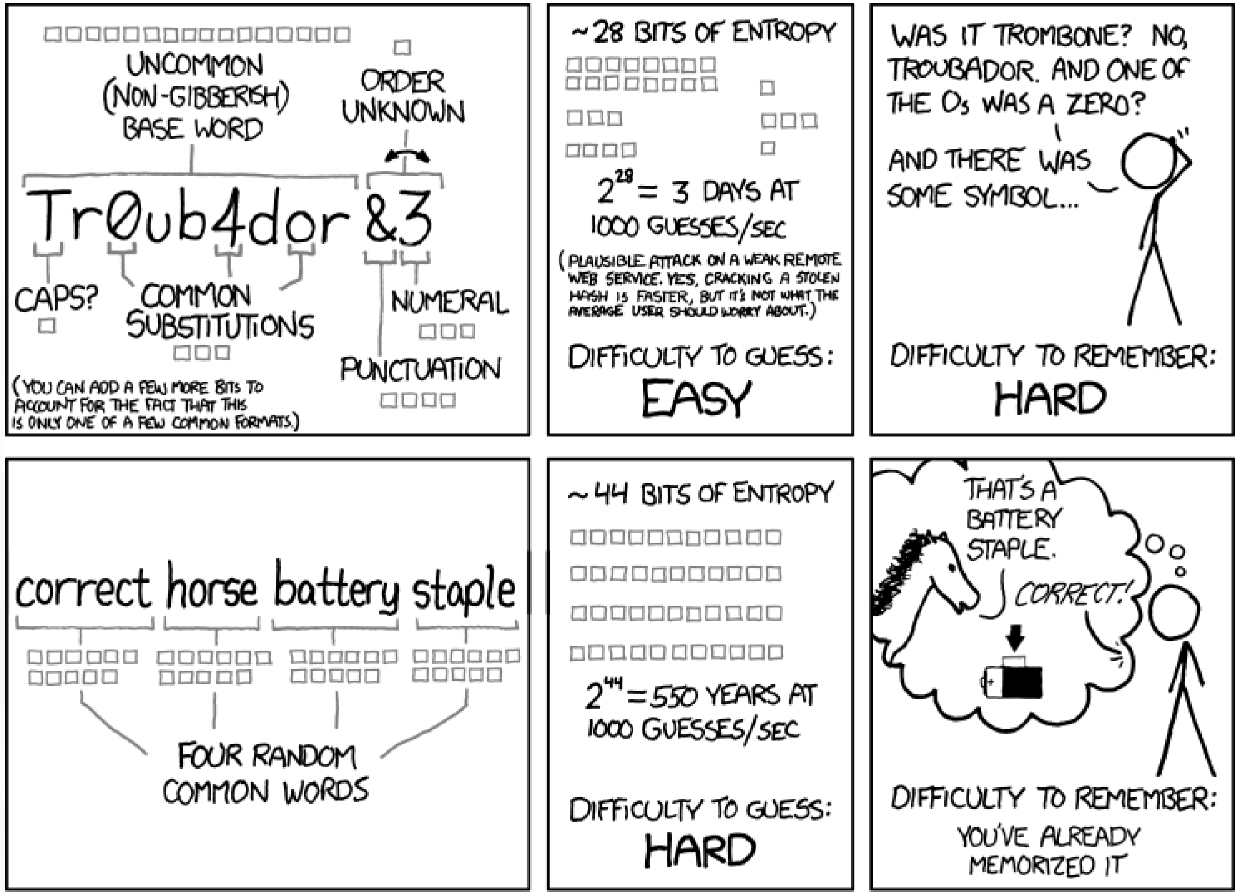
- Offline brute-force guessing of passwords using a dictionary or character patterns
- Used to recover plaintext passwords from encrypted files and network traffic



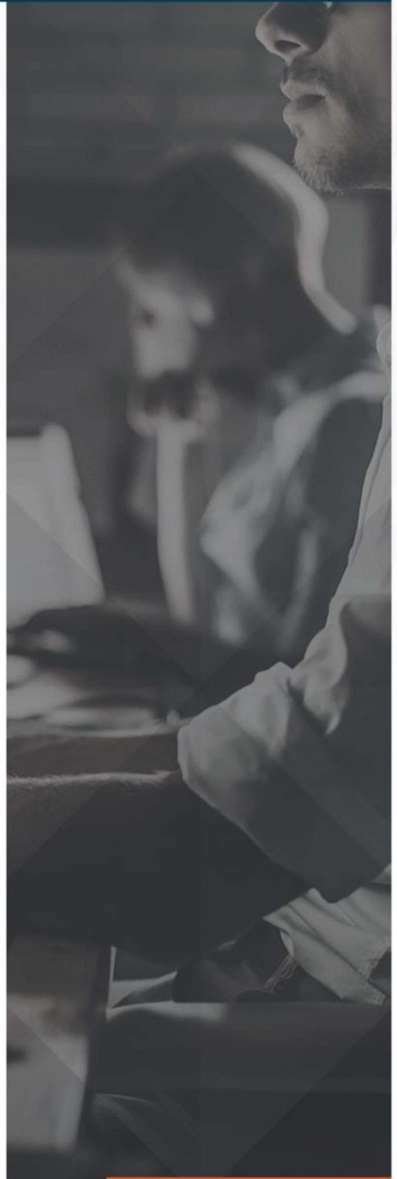
```
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Type........: MD5
Hash.Target......: 0301hashes.txt
Time.Started.....: Wed Aug 01 07:10:48 2018 (12 secs)
Time.Estimated...: Wed Aug 01 07:12:02 2018 (1 min, 2 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Mod........: Rules (best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#2.....: 14849.2 kH/s (6.88ms)
Recovered........: 3/7 (42.86%) Digests, 0/1 (0.00%) Salts
Progress.........: 179463438/1104427170 (16.25%)
Rejected.........: 5390/179463438 (0.00%)
Restore.Point....: 2330694/14343210 (16.25%)
Candidates.#2....: 2010mt -> 1pl123
HWMon.Dev.#2.....: N/A
```



THE FIX: LONG PASSWORDS (PASSPHRASES)

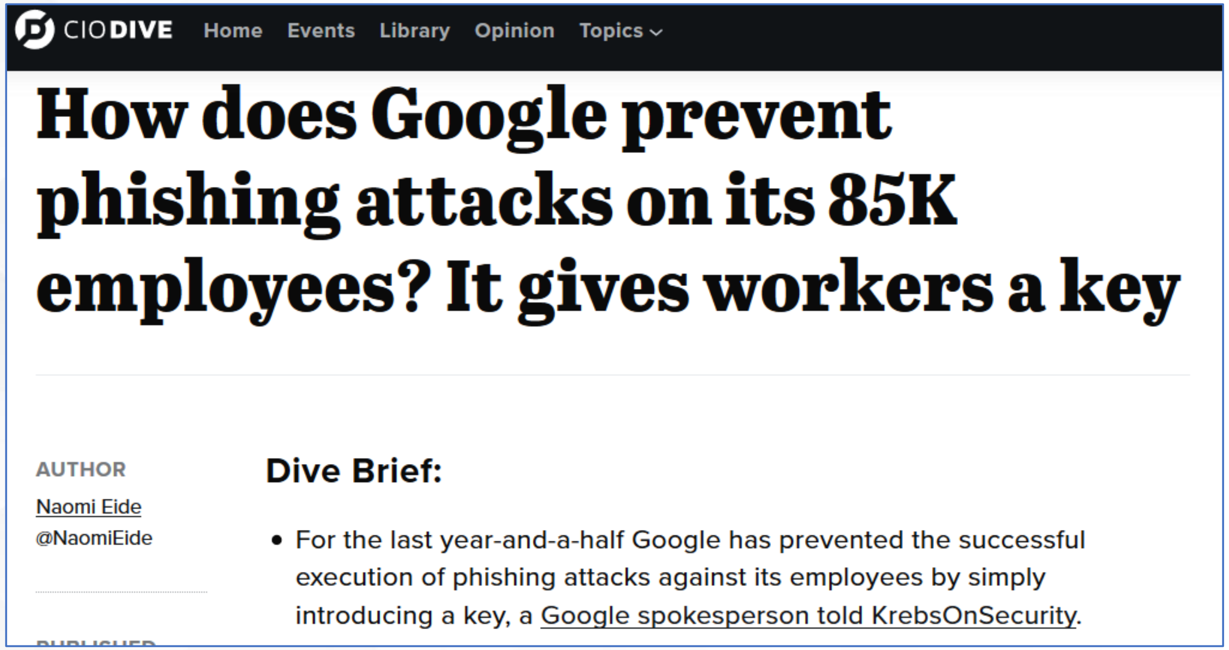

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



MULTI-FACTOR AUTHENTICATION

- There are many cost-effective, non-invasive solutions available today



CIODIVE Home Events Library Opinion Topics

How does Google prevent phishing attacks on its 85K employees? It gives workers a key

AUTHOR

Naomi Eide
@NaomiEide

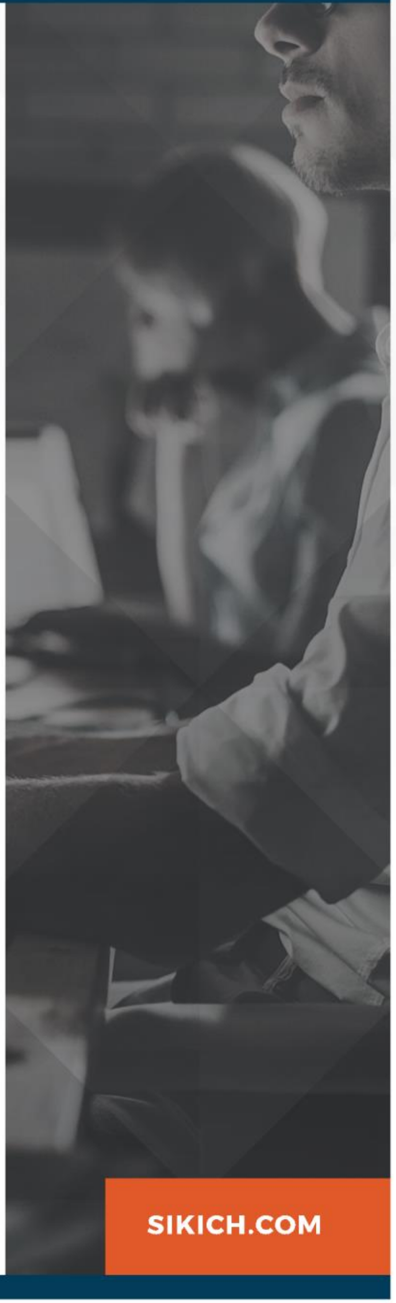
PUBLISHED

Dive Brief:

- For the last year-and-a-half Google has prevented the successful execution of phishing attacks against its employees by simply introducing a key, a Google spokesperson told KrebsOnSecurity.

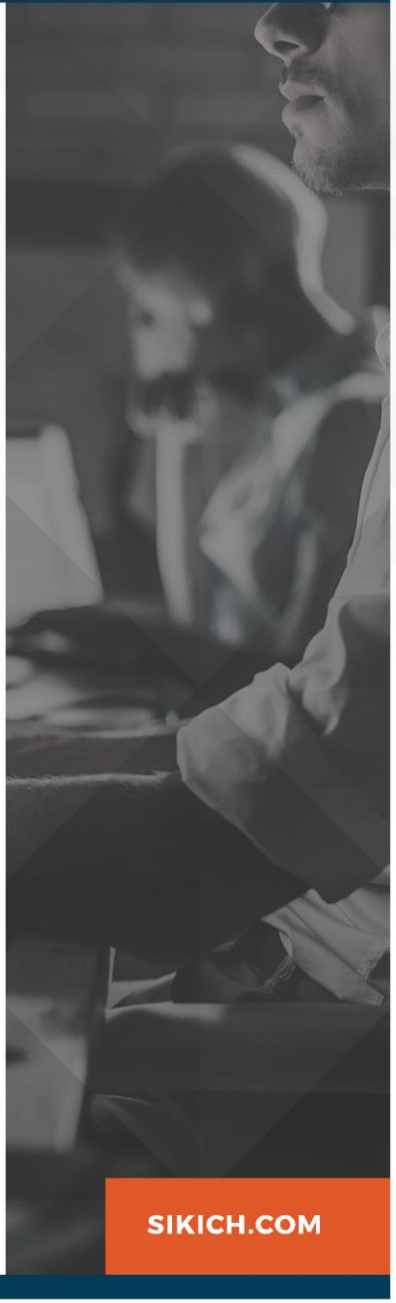
AGENDA

- Hackers and Breaches
- Monetizing Breaches
- Incident Response and Forensics
- Password Considerations
- **INDICATORS OF INFOSEC PROGRAM MATURITY**



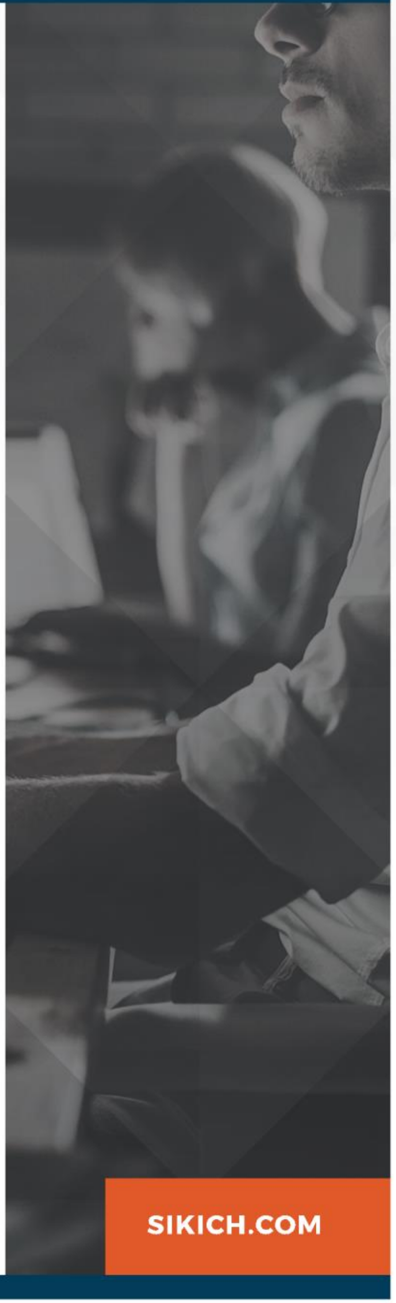
AUTOMATED PATCHING

- Does your college have a centralized system for deploying and monitoring security patches?
- Does your college automate patching for third-party applications (such as Adobe Reader, Java, Firefox and Chrome?)
- This can be difficult with so many different systems!



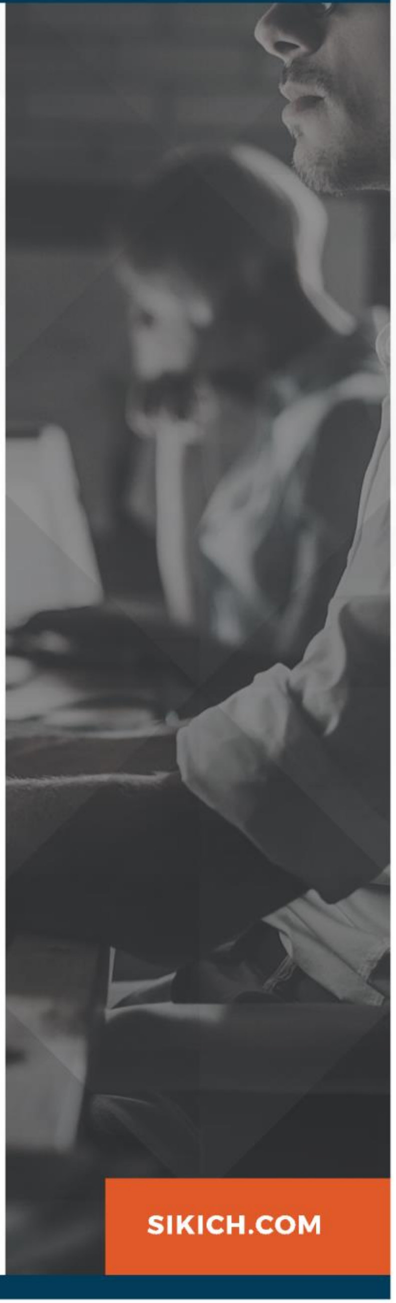
CENTRALIZED ANTI-VIRUS

- Is there a central console to monitor anti-virus coverage and alerts?
- Does the College enable advanced anti-virus features?
  - Behavioral detection
  - Software firewall
  - Host-based intrusion detection
  - Device control/lockdown
- It is possible to provide free AV for students.



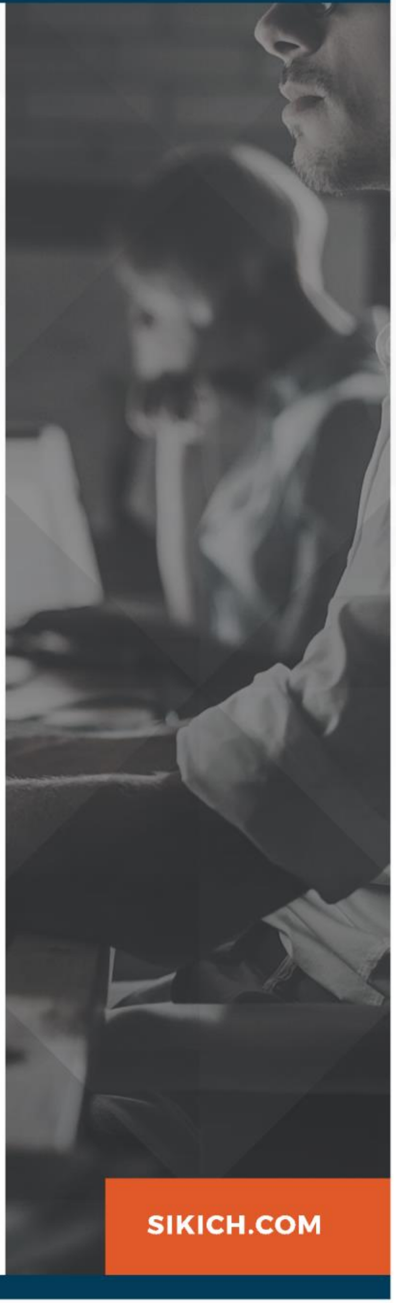
PASSWORD PRACTICES

- Are long or complex passwords enforced?
- Does the college train employees and students about the risks of weak password practices?
  - Guessable patterns
  - Password re-use on different systems
  - Formal training for faculty and staff
  - A simple newsletter for students.



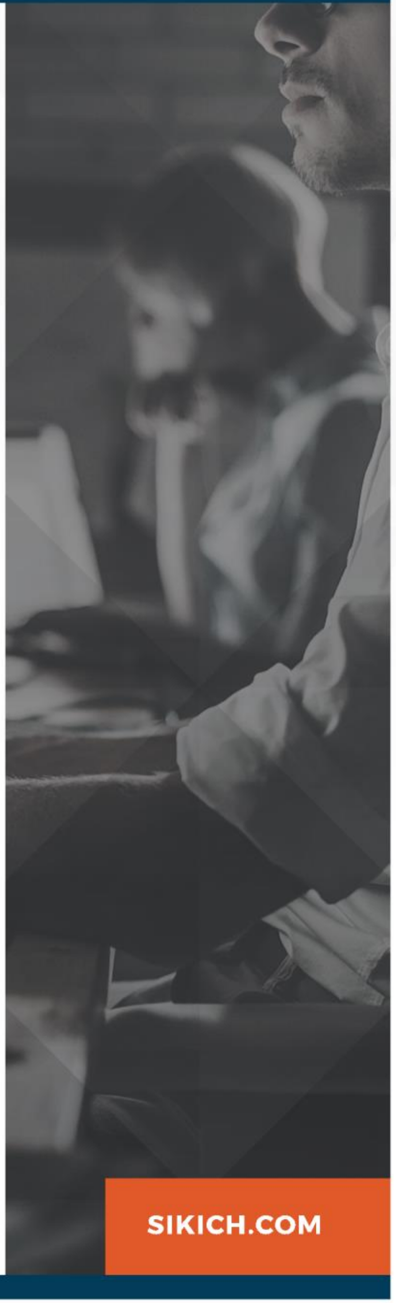
BACKUPS AND DATA MANAGEMENT

- Does the college allow important data on laptops without backups?
  - Should not be done at all. Use a secure Cloud.
- Does the college's IT department conduct periodic disaster recovery testing?
- Does the college have a network share that is a "dumping ground" to which all faculty and staff have rights?
- Are faculty and staff using cloud services (such as Google Docs) for work without IT oversight?



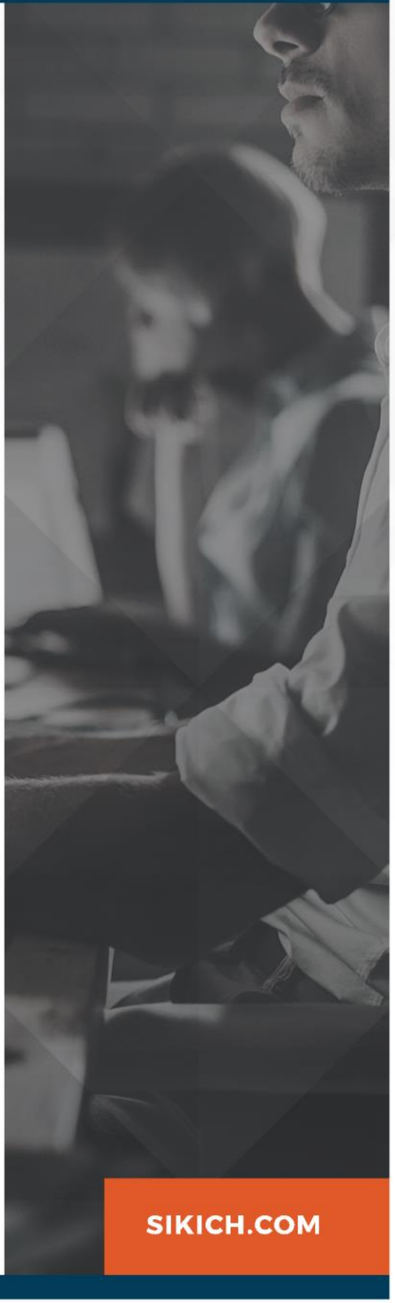
WEB FILTERING

- Does the college have web filtering in place?
- Effective web filtering provides numerous benefits
    - Can block phishing sites/drive-by malware downloads
    - Keeps employees on task
    - Helps reduce complaints of harassment or inappropriate use
    - Can block malware C&C channels
    - Freedom of speech vs safety



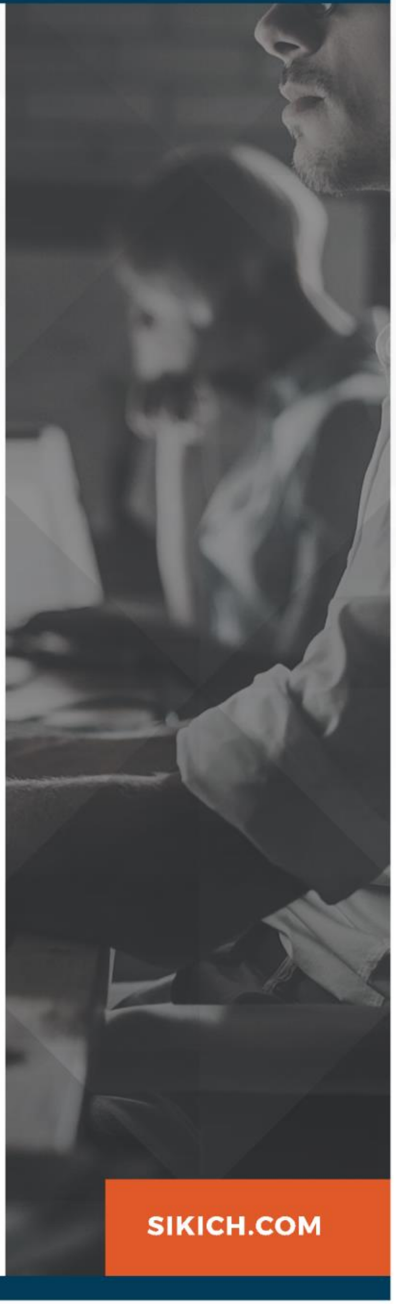
MULTI-FACTOR AUTHENTICATION FOR REMOTE ACCESS

- Does the college require multi-factor authentication for VPN and remote desktop access?
- Colleges are increasingly deploying multi-factor authentication for email, external application and cloud storage access as well
- Focus here on faculty and staff.
  - Can get bombarded with support calls if rolled out to students.



SYSTEM HARDENING

- Does your college run end-of-life systems, such a Windows XP and Windows 2003?
  - Sometimes needed for research BUT they should be on their own network and have no access to file shares, etc.
- Does the college have a standard/automated build process for workstations?
  - Does it reset when a student logs off a public computer?

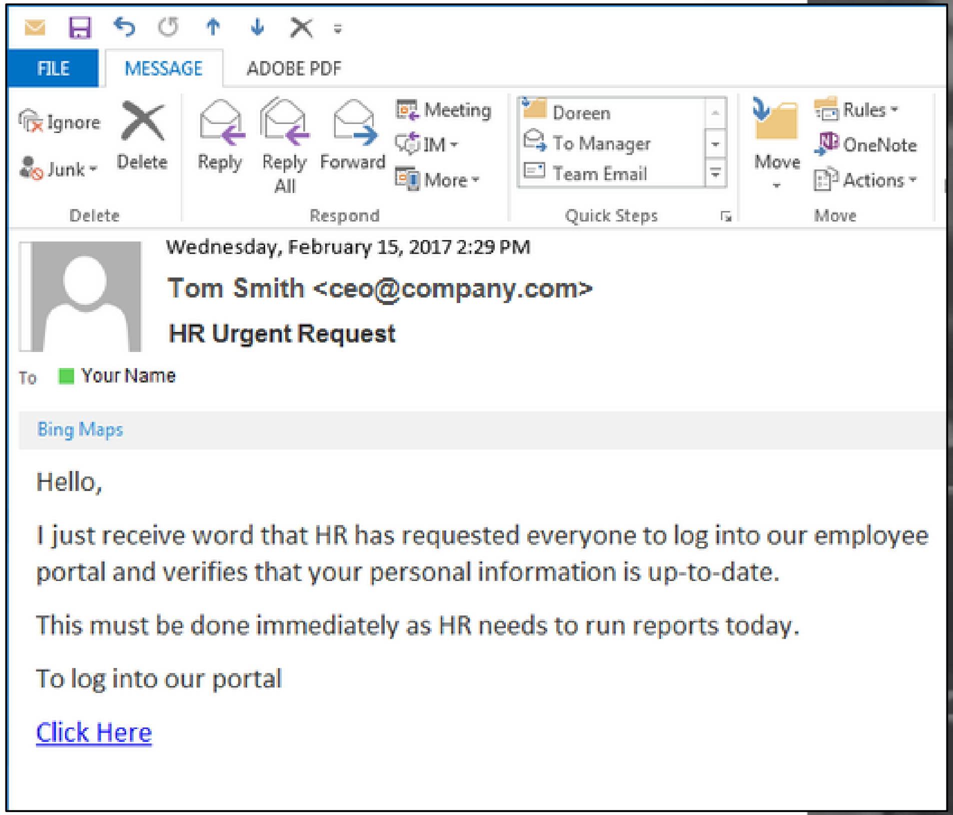


SOCIAL ENGINEERING AND PHISHING

- Mistakes often lead to incidents
  - Phishing or pretext calling may lead to electronic payment fraud
  - Physical intrusions or “tailgating” can lead to keyloggers and rogue network devices
- Best defense is policies/procedures, education and enforcement

PHISHING EXERCISES

- There are a number of cloud service providers for periodic phishing exercises
- These activities have been shown effective at reducing risky "click through" rates of employees



Wednesday, February 15, 2017 2:29 PM

Tom Smith <ceo@company.com>

HR Urgent Request

To Your Name

Hello,

I just receive word that HR has requested everyone to log into our employee portal and verifies that your personal information is up-to-date.

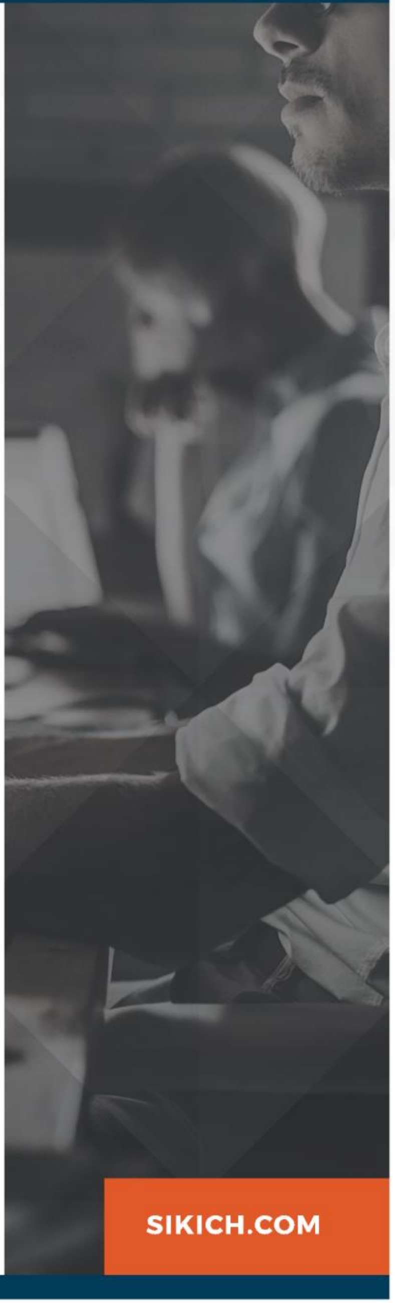
This must be done immediately as HR needs to run reports today.

To log into our portal

Click Here

THIRD-PARTY ASSESSMENT OF SECURITY POSTURE

- IT Controls Audit
  - List the organization’s control objectives and controls
  - Evaluate the appropriateness and execution of the controls
- Framework Audit
  - Assess the organizations controls against an industry or regulatory checklist
- Risk Assessment
  - “Thought exercise” type assessment considering threats, controls and control effectiveness
- Network Security Assessment
  - Automated and manual collection of vulnerability and configuration data to assess the organization’s posture
- Penetration Test
  - Simulation of a real-world attack



THANK YOU FOR YOUR TIME.

Are there any questions?

John Thomas

John.Thomas@sikich.com

877.403.5227

SIKICH.COM

SIKICH®

ACCOUNTING TECHNOLOGY ADVISORY

LinkedIn: www.linkedin.com/company/sikich
Facebook: www.facebook.com/sikichllp
Twitter: www.twitter.com/sikichllp
Blog: www.sikich.com/blog

SIKICH.COM