

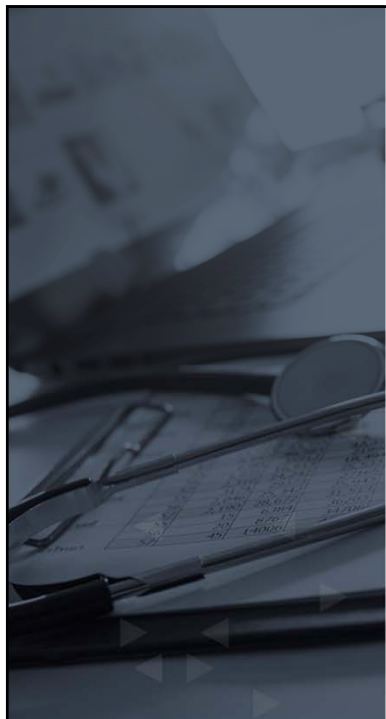


THOUGHTWARE®

Health Care

BKD
CPAs & Advisors

Everyone needs a trusted advisor. Who's yours?



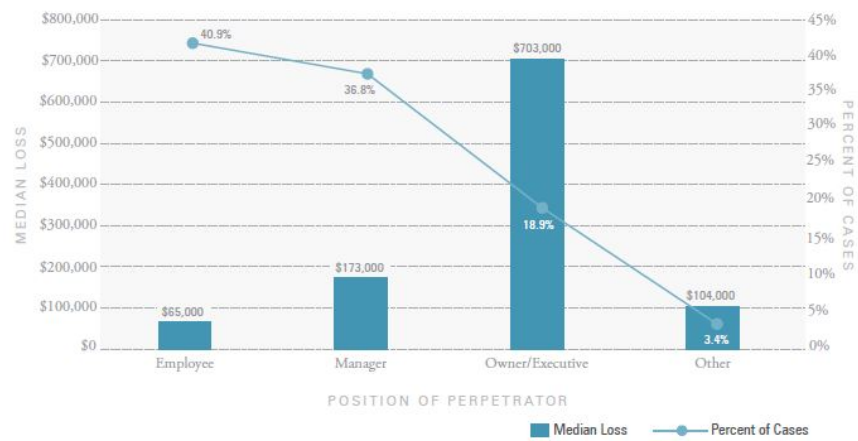
The Psychology of Fraud & Stupid Human Tricks

Rand Gambrell, Director, Forensics & Valuation Services
Rick Lucy, Director, IT Risk Services

September 27, 2019

BKD

Figure 65: Position of Perpetrator—Frequency and Median Loss



BKD

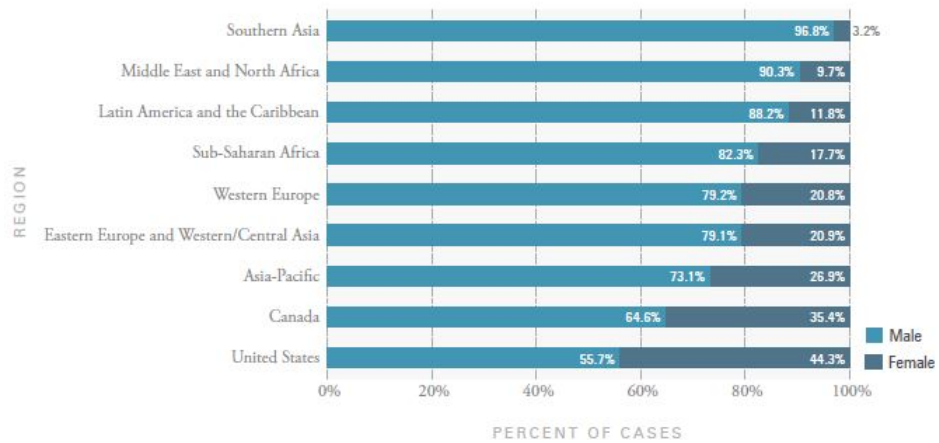
Figure 78: Frequency of Schemes Based on Perpetrator's Department

Department/ Scheme	Accounting	Operations	Sales	Executive/Upper Management	Customer Service	Purchasing	Finance	Warehousing/ Inventory
Cases	348	312	260	228	189	161	94	86
Billing	27.0%	21.5%	14.2%	36.8%	9.5%	25.5%	24.5%	9.3%
Cash Larceny	14.9%	7.7%	8.1%	10.1%	14.3%	3.7%	18.1%	0.0%
Cash on Hand	15.5%	13.8%	6.5%	12.3%	18.5%	13.0%	22.3%	5.8%
Check Tampering	30.5%	9.3%	2.7%	13.6%	7.4%	6.2%	24.5%	1.2%
Corruption	21.6%	34.9%	34.6%	50.0%	25.4%	66.9%	37.2%	32.6%
Expense Reimbursements	15.8%	12.2%	14.2%	23.7%	5.8%	14.9%	14.9%	3.5%
Financial Statement Fraud	12.9%	5.4%	7.3%	30.3%	3.7%	3.1%	23.4%	9.3%
Non-Cash	7.2%	19.6%	20.4%	24.6%	16.4%	18.6%	13.8%	57.0%
Payroll	21.6%	6.4%	1.5%	10.1%	3.7%	5.0%	7.4%	2.3%
Register Disbursements	3.2%	4.2%	5.0%	1.8%	3.2%	4.3%	3.2%	0.0%
Skimming	17.5%	12.8%	11.9%	11.8%	16.9%	7.5%	12.8%	5.8%

Less Risk More Risk

BKD

Figure 80: Gender of Perpetrator Based on Region



The Usual (?) Suspects



Everyone needs a trusted advisor.
Who's yours?

BKD

Bernie Madoff

- \$65 billion Ponzi scheme
- Lasted over 15 years, during which Madoff was investigated at least 8 times by the SEC
- More than 51,700 claims filed by alleged victims



Everyone needs a trusted advisor.
Who's yours?

BKD

Toby Groves



- Founder of Groves Funding Corporation
- Misrepresented income, falsified loan documents, reported fictitious homes
- \$7 million bank fraud

Everyone needs a trusted advisor.
Who's yours?

BKD

Anonymous

- Anti-Cyber Surveillance
- Anti-Cyber Censorship
- Internet Activism
- Internet Vigilantism



9

Everyone needs a trusted advisor.
Who's yours?

BKD

Why do good (?) people do bad things?

**BKD**

Classic Theories of Fraud Motivation



- Edwin H. Sutherland and “Differential Association”
 - Criminal behavior is learned through interaction with others, not through institutions
 - Fails to address WHY people adopt criminal behavior

Everyone needs a trusted advisor.
Who's yours?

BKD

THE FRAUD TRIANGLE

Pressure
Motivation or Incentive to
Commit Fraud

Rationalization
Justification of Dishonest
Actions

FRAUD

Opportunity
The Knowledge and Ability
to Carry Out Fraud

BKD

The Fraud Diamond

The person with Capability

- Position and authority in the organization
- High level understanding of system
- Egoistic nature
- Persuasive & deceptive nature
- Resilience to stress



Everyone needs a trusted advisor.
Who's yours?

BKD

Breaking Bad ... A Case Study in Criminal Behavior



- Walter White
 - Terminally Ill with minimal financial resources (perceived need)
 - Former student is involved in drug underworld (perceived opportunity)
 - Walter is not a “bad guy,” he’s just doing this for his family (rationalization)

Everyone needs a trusted advisor.
Who's yours?

BKD

Current Fraud Theory – Reversal Theory

- Motivation is divided into four polarities (each with a choice):
 1. Rules – conform or rebel?
 2. Task – get the job done or enjoy the journey?
 3. Who benefits – me or others?
 4. Who grows – do I gain mastery or do I help others?



Everyone needs a trusted advisor.
Who's yours?

BKD

The Values of the Eight Motivational States

Source: © Apter International. Used with permission.



Everyone needs a trusted advisor.
Who's yours?

BKD

Impact on Fraud Motivation

1. Serious – need for money due to dire financial circumstances
2. Playful – the thrill of the chase
3. Conforming – everyone is doing it
4. Rebellious – the pleasure of being bad
5. Mastery – beating the system
6. Sympathy – a form of self-indulgence
7. Self – personal gain
8. Other – using gains for one's family

Everyone needs a trusted advisor.
Who's yours?

BKD

The Practical Impact of Reversal Theory?



Everyone needs a trusted advisor.
Who's yours?

BKD

What About Co-Conspirators?



- Often, co-conspirators aren't bad people, they can't see the impact (fraud is *unintentional*)
- People commit fraud because of relationships (we like each other)
- Cognitive association limitations

Everyone needs a trusted advisor.
Who's yours?

BKD

Toby Groves Revisited



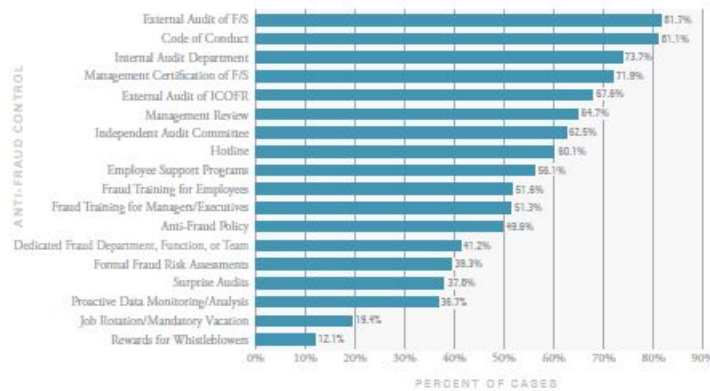
- Founder of Groves Funding Corporation
- Misrepresented income, falsified loan documents, reported fictitious homes
- \$7 million bank fraud
- Why did employees, title company personnel, etc. contribute to the fraud?

Everyone needs a trusted advisor.
Who's yours?

BKD

The Future of Fraud Controls

Figure 47: Frequency of Anti-Fraud Controls



Everyone needs a trusted advisor.
Who's yours?

BKD

And Now, Stupid Human Tricks (aka Managing Cyber Risk)

Rick Lucy, IT Risk Services Director



Everyone needs a trusted advisor. Who's yours?


[Send a Release](#)

32 Million Breached Patient Records in First Half of 2019 Double Total for All of 2018

NEWS PROVIDED BY
Protenus →
 Jul 31, 2019, 13:51 ET

SHARE THIS ARTICLE








23

Everyone needs a trusted advisor. Who's yours?





xtelligent HEALTHCARE MEDIA

[Home](#)
[News](#)
[Features](#)
[Interviews](#)

[HIPAA and Compliance](#)
[Cybersecurity](#)
[Cloud](#)
[Mobile](#)
[Patient Privacy](#)
[Data Breaches](#)

CYBERSECURITY NEWS

Data Breaches Cost Healthcare \$6.5M, or \$429 Per Patient Record

Breach costs are rising, with healthcare spending more than all other sectors for the ninth consecutive year at \$6.5 million on average, an IBM-sponsored Ponemon Institute report shows.

24

Everyone needs a trusted advisor. Who's yours?



- **Compliance does not equal security:**

- But it sure does help – *Greg Masters, SC Media*
- There's an industry fallacy in that we believe that once we meet compliance, we're good. – *Joey Smith, CISO, Schnucks Markets*

- The threats you **think** you face may be vastly different than the threats that **actually** pose the greatest risk.
- As IoT devices become targets, healthcare organizations need to shift their way of thinking. Health systems must segment the networks to ensure only authenticated users have access to such devices.

200 Million Devices Vulnerable to Remote Takeover Via VxWorks Flaw

Armis found 11 critical vulnerabilities in the VxWorks system, a platform found in 2 billion devices, including medical equipment and IoT devices; officials say patching will be long and difficult.

25

Everyone needs a trusted advisor. Who's yours?

BKD CYBER

INTERNET OF THINGS

**BKD**

nu
Q Search
Bloomberg
Sign In
Subsc

Cybersecurity

Cyber Risks to Exceed Natural Disasters for Insurers: Scor CEO

By [Helene Fouquet](#) and [William Horobin](#)
May 10, 2019, 8:07 AM MDT Updated on May 10, 2019, 11:20 AM MDT

- ▶ Re-insurer CEO Kessler says sector must build coverage system
- ▶ ECB calls on financial firms to conduct cyber stress tests


SHARE THIS ARTICLE

- Share
- Tweet
- in Post
- Email

Cyber risks will soon become bigger risks than natural catastrophes for the insurance sector, Scor Chairman and Chief Executive Officer Denis Kessler said, recommending the industry build a comprehensive, common global scale to assess cyber-related incidents.

LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >
Bloomberg Television

27
Everyone needs a trusted advisor. Who's yours?
BKDCYBER



CYBER THREATS

- The biggest threats to your assets are actually the same old threats that we were worried about last year, five years ago, and in many cases even a decade ago.
- Only a handful of attacks truly use sophisticated "Mission Impossible" techniques.
- When a criminal is trying to hack an organization, they won't re-invent the wheel unless they absolutely have to.
- Cyber criminals tend to seek the highest returns in the shortest time with the least risk.
- Cyber criminal organizations are successful because they are generally well funded, they have the technical resources to create new and increasingly more capable attack methods, and they often are highly collaborative in nature.

28
BKD



CYBER THREATS

29

- According to IBM's "Cyber Security Intelligence Index" 95% of all security incidents **prey on human weakness** in order to lure insiders within organizations to unwittingly provide them with access to sensitive information.
- 59% of respondents agree that most information technology security threats that directly result from insiders are the result of **innocent mistakes** rather than malicious abuse of privileges.

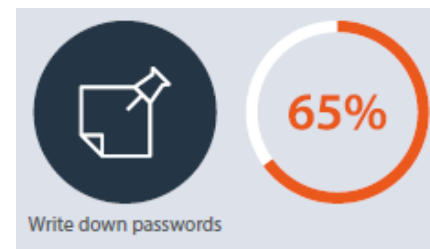
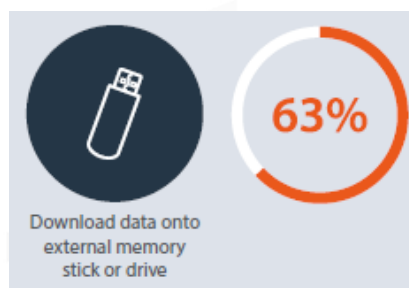
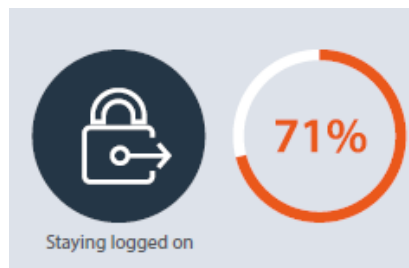
BKD



CYBER THREATS

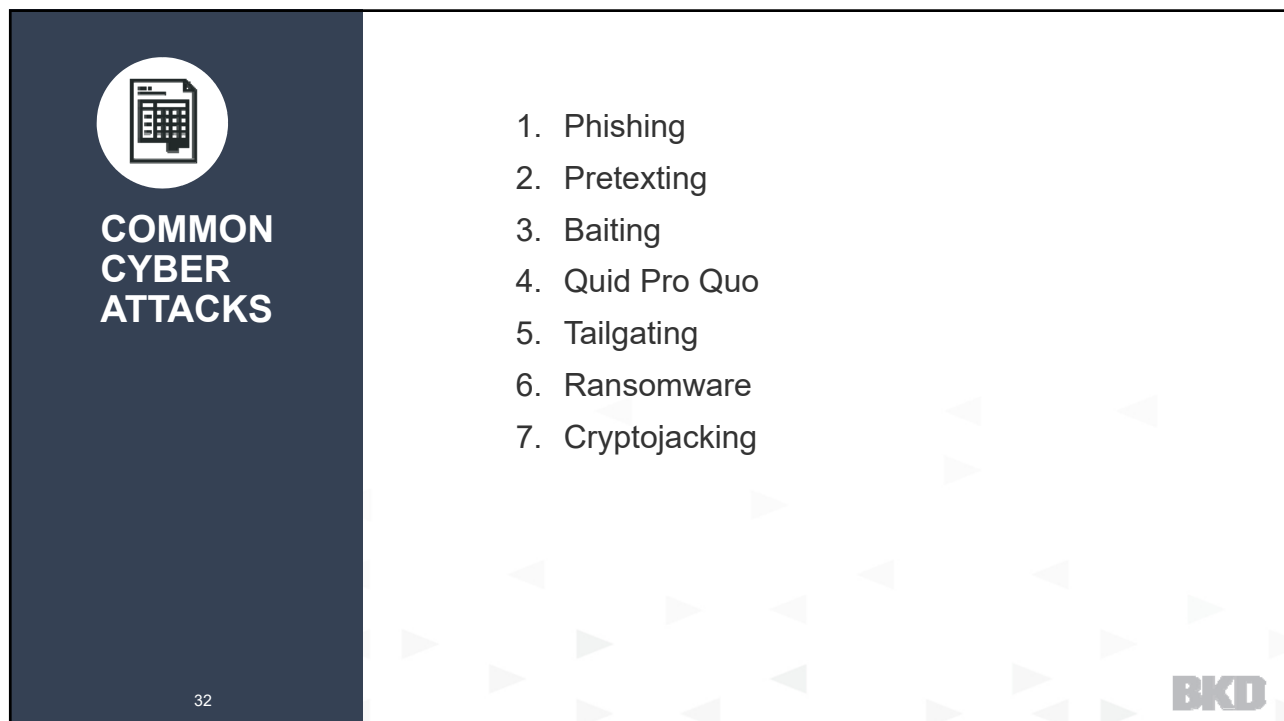
Insider Risks

30



Bogmar Privileged Access Threat Report 2018

BKD





PHISHING

33

- Phishing is the crafting of a message that is sent typically via email and is designed to influence the recipient to “take the bait” via a simple mouse click.
- Seek to obtain personal information, such as names, addresses and social security numbers.
- That bait is most often a **malicious attachment** but can also be a link to a page that will request credentials or drop malware.

BKD



PHISHING

34

- May use **link shorteners** or embed links that redirect users to suspicious websites in URLs that appear legitimate. (Bitly, TinyURL, Ow.ly, etc.)
 - From: <https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>
 - To: <https://ibm.co/1PO3b9x>
- Fake/disposable e-mail address generators
 - Yahoo Mail, Dispostable, GuerrillaMail, SpamBog, GMX, etc.
- Messages tend to incorporate **threats, fear and a sense of urgency** in an attempt to manipulate the user into acting promptly.

BKD



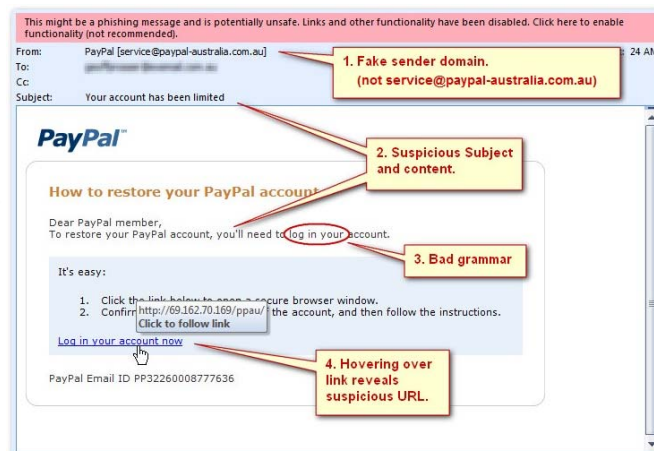
PHISHING

35

- Some phishing emails are poorly crafted and **exhibit spelling and grammar errors**.
- In a normal organization, **78% of people don't click** a single phish all year. That's pretty good news.
- On average in any given phishing campaign **4% of people will click it**--the vampire only needs one person to let them in.
- **Only 17% of phishing campaigns were reported**. Additional training should also be bestowed on users that don't report the phishing!

BKD

PHISHING EXAMPLES



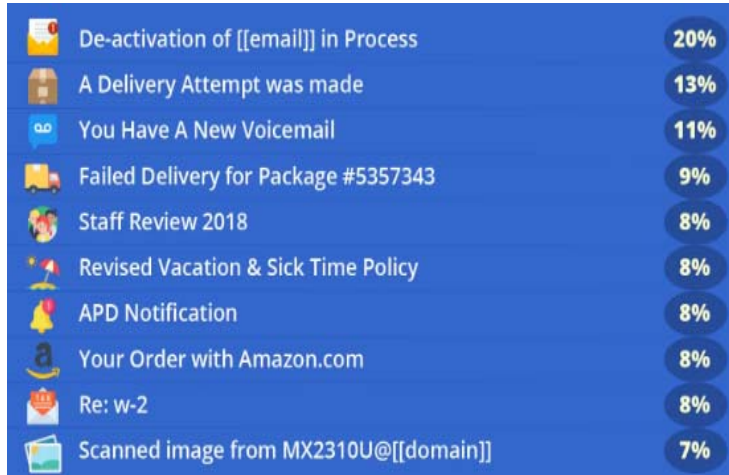
BKD



PHISHING

37

KnowBe4's "Top 10 Global Phishing Email Subject Lines for Q1 2019"


<https://www.knowbe4.com>

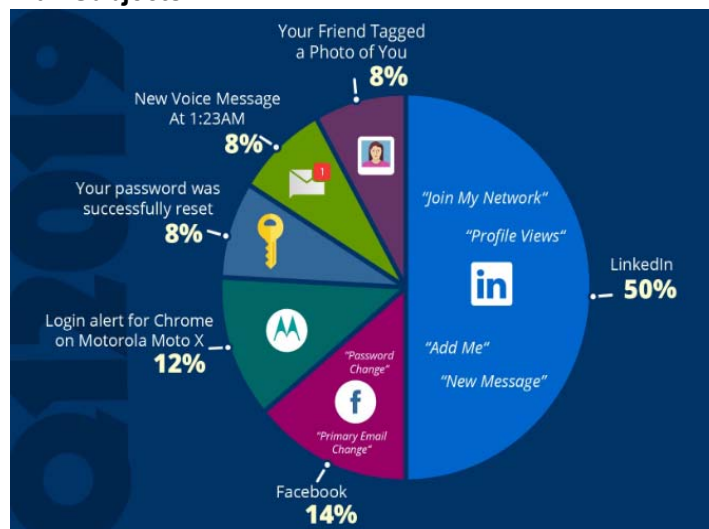
BKD



PHISHING

38

KnowBe4's "Top-Clicked Phishing Tests – Social Media Email Subjects"


<https://www.knowbe4.com>

BKD



PRETEXTING

39

- Pretexting is the **creation of a false narrative** to obtain information or influence behavior.
- Could be a phone call, text message, email, etc. designed steal the victims' personal information.
- Scammer pretends that they need certain bits of information from their target in order to confirm their identity.
- Pretexting may also involve impersonating co-workers, police, bank, tax authorities, clergy, insurance investigators, auditors, etc.

BKD

PRETEXTING EXAMPLE

E-mail based

From: "Bank of America" customerservice@bankofamerica.com
 To: "Jane Smith" jane-smith12@gmail.com
 Date: Wed, May 26, 2010
 Subject: Fraud Alert – Action Required



Dear Customer,


At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, [sign up now](#). New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department 

BKD

PRETEXTING EXAMPLE

Phone based

- New credit card.
- Past due bill/collection call.
- Delinquent taxes.

BKD

BAITING

- Baiting is the promise of an **item or good** that hackers use to entice victims to get login credentials to a certain site.
- Baiting attacks are not restricted to online schemes. Attackers can deliver malware via the use of physical media.
- Many people will pick up USBs and plug them into their computers without thinking.
- The USBs may automatically activate a keylogger that allows access to observe an employee's online activity and login credentials or install malware.

BKD



BAITING

43

FEDERAL TRADE COMMISSION
Consumer Information

[MONEY & CREDIT](#) [HOMES & MORTGAGES](#) [HEALTH & FITNESS](#) [JOBS & MAKING MONEY](#) [PRIVACY, IDEN ONLINE SECUF](#)

[Home](#) > [Blog](#)

Get a one-ring call? Don't call back.

Share this page [f](#) [t](#) [in](#)

May 7, 2019
by Michael Atleson
Acting Assistant Director, Division of Consumer & Business Education

A while back, we warned you about the “one ring” scam. That’s when you get a phone call from a number you don’t know, and the call stops after just one ring. The scammer is hoping you’ll call back, because it’s really an international toll number and will appear as a charge on your phone bill — with most of the money going to the scammer. Well, the scam is back with a vengeance, and the FCC just issued a new [advisory](#) about it. Read the FCC’s advisory for more detail, but the advice from both agencies remains the same if you get one of these calls:

BKD



QUID PRO QUO

44

- The Quid Pro Quo usually **assumes the form of a service**, whereas Baiting frequently takes the form of a good.
 - One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find.
 - These attackers offer IT assistance to each and every one of their victims.
 - Eventually you will reach someone with a legitimate problem.
 - The user will be grateful you called and will eagerly follow your instructions.
 - The fraudsters will promise a quick fix in exchange for the employee disabling their AV program that assumes the guise of software updates.
 - The attacker then gets the user to install malware on their computer.
- BKD**



TAILGATING

- Another social engineering attack type is known as tailgating or “piggybacking.”
- These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area.



45

BKD



RANSOMWARE

- Attacks are inevitable.
- Around half of business victims pay the ransom.
- Most are able to retrieve data after payment.
- Many would pay again.
- Ransomware will continue to be one of the most prevalent attacks.
- Perpetrators are being greatly assisted by the emerging **Ransomware as a Service (RaaS)**



46

BKD

RANSOMWARE

Healthcare Examples

5 More Healthcare Providers Fall Victim to Ransomware Attacks

Last week, Colorado-based NEO Urology paid a \$75,000 ransom to unlock its systems; since then, another five providers reported ransomware attacks that drove many to pen and paper.



Estes Park Health (EPH) in Colorado has suffered a ransomware attack that resulted in widespread file encryption across the network.

The attack was noticed by employees on Sunday June 2, 2019 who reported that their computers were behaving strangely. EPH contacted its on-call IT technician who logged in and experienced the same issues, as the ransomware systematically encrypted files on the network. EPH, Chief Information Office, Gary Hall, witnessed the ransomware locking files and taking control of programs on his computer, according to a recent report in the *Estes Park Trail Gazette*.

According to the Telstra Security Report 2018, four out of five ransomware victims who paid a ransom to recover their files said they would pay the ransom again to recover data if no backup files are available.

BKD

RECOMMENDATIONS

The Basics

Inventory

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?


BKD

RECOMMENDATIONS

The Basics

Educate

- Technology is no substitute for employee education.
- Educate and re-educate the entire organization, not just IT.
- Include the Board, Executives and Vendors.
- Knowledge is power.
- Do not discourage false-positive reporting.
- Document your security policies in a knowledge database so that everyone understand exactly what is going on – and why.
- Develop and rehearse a robust incident response program.

BKD

RECOMMENDATIONS

The Basics

Patch

- Applications
- Databases
- Operating systems – servers, workstations, etc.
- Anti-virus/Anti-malware – engines and signatures.
- Third-party applications.

BKD

RECOMMENDATIONS

Limit

- Control use of administrative privileges.
- Limit access based on need-to-know (least privilege).
- Limit and control remote access.
- Do not share credentials. Consider a password safe.
- Consider multi-factor authentication.
- Limit the use of portable media.

BECKER'S
HEALTH IT & CIO REPORT

Colorado hospital to pay \$111K HIPAA settlement

Jessica Kim Cohen - Wednesday, December 12th, 2018 [Print](#) | [Email](#)

[SHARE](#) [Tweet](#) [Share 4](#)

Pagosa Springs (Colo.) Medical Center has agreed to pay \$111,400 to the HHS Office for Civil Rights and adopt a corrective action plan to settle allegations that it failed to terminate a former employee's access to protected health information held online.

The settlement resolves a complaint alleging that a former employee of Pagosa Springs Medical Center continued to have remote access to the critical access hospital's web-based scheduling calendar, which contained patients' protected health information.

BKD

RECOMMENDATIONS

The Basics

Check

- Lock down everything that is not needed.
- Generate logs and review them. Don't forget to document your review.
- Escalate potential security issues.
- Limit and monitor vendor access.
- Filter out suspicious email addressed to employees.
- Implement a policy for dealing with suspected phishing and pretexting.

BKD

RECOMMENDATIONS

The Basics

Prevent

- Lock your laptop whenever you are away from your workstation.
- Do not give out personal or company confidential information on the phone, through the mail or over the Internet unless you have initiated the contact or know who you are dealing with.
- Monitor in and outbound traffic for unusual patterns.
- Encrypt data at rest and in motion. Don't just protect the perimeter (firewall), also protect the data.
- Segment critical data. Encrypt data within crown-jewel segments.

BKD

RECOMMENDATIONS

The Basics

Backup

- Implement a regularly scheduled backup program that meets your business and records retention requirements.
- Put some distance between your primary and secondary sites.
- For critical applications, perform a full restoration or fail-over test at least annually.
- Backup and restore **not only data, but also the applications.**
- Understand the differences between cloud storage and cloud backup.

BKD

CLOSING THOUGHTS

Call to Action

- Perform a framework-based, cybersecurity assessment that allows the organization to determine the organization's assets to protect, compliance requirements and cyber-readiness of current protections
- Remediation activities should be prioritized and scheduled over time, based on level of risk
- Build a robust breach/incidence response plan that is practiced and updated regularly

BKD

POP QUIZ!

Question 1

Your supervisor is very busy and asks you to log into the HR server using her user-ID and password to retrieve some reports. What should you do?

- A. It's your boss, so it's okay to do this.
- B. Ignore the request and hope she forgets.
- C. Decline the request and remind your supervisor that it is against policy.

**BKD**

POP QUIZ!

Question 2

You receive the following email from the Help Desk. What should you do?

Dear Email User, Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed. *Name (first and last): *Email Login: *Password: *Date of birth: *Alternate email:

Please contact the Webmail Team with any questions. Thank you for your immediate attention.

A. Reply back to the email immediately so your account will not be deleted.

B. Don't respond to the email, instant messages, texts, phone calls, etc., asking you for your password or other private information.



C. Notify the Help Desk or IT Dept that you received this email.

**BKD**

POP QUIZ!

Question 3

A friend sends an electronic Hallmark greeting card to your work email. You need to click on the attachment to see the card. What should you do?

A. The email address looks like it came from Hallmark, so it's OK to click the link.

B. The email message is electronically signed by my friend, so it is OK to click the link.

C. Delete the email.

**BKD**

POP QUIZ!**Question 4**

All of these are good physical security practices except?

A. Always wear your security badge when leaving work, even if just for a break. They should be worn outside of the office in public so other people know where you work.



B. Control access to your office by ensuring the door closes completely when entering and exiting. Ensure that no one slips in behind you.

C. When working in a public setting, prevent shoulder surfing by shielding your paperwork and keyboard from view using your body.

D. Follow the Clear Desk and Screen Policy. Store confidential and sensitive items securely.

BKD**POP QUIZ!****Question 5**

How are passwords like bubble gum?

A. They are strongest when fresh.

B. They should not be shared by a group.

C. If you leave them laying around, there's a good chance you'll have a sticky mess.

D. All of the above.

**BKD**



CYBER DEFENSE

61

Forbes

Billionaires Innovation Leadership Money Consumer Industry Lifestyle Bran

With Immediate Physical Action In A World First



Kate O'Flaherty Senior Contributor @
Cybersecurity
I'm a cybersecurity journalist.

f
t
in



As the number and severity of cyber attacks continue to rise, what actions are you taking to minimize the risk of a cyber attack?

BKD

WHAT IS THE RIGHT AMOUNT OF SECURITY?



This much

BKD

Questions?

Rand Gambrell, BKD FVS Director
303-837-3594, rgambrell@bkd.com

Dr. Rick Lucy, BKD IT Risk Director
303-861-4545, rlucy@bkd.com



Thank You!

