The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina. Consult your attorney for advice concerning specific situations.

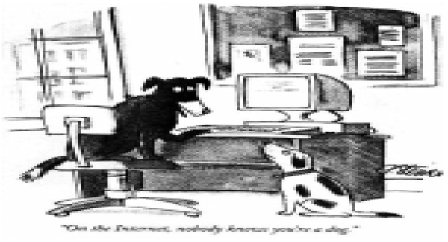
People, Policies, and Technology:

Protecting Information in a Connected World

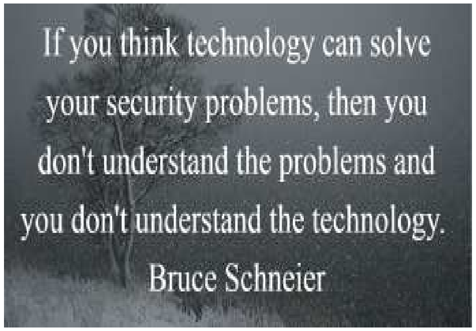
September 4, 2019

Challenges of a Connected World

- The Internet was not designed with security in mind
- Computers and computer networks default to open
- On the Internet, No One Knows You Are a Dog.



No Technology Tool Can Keep All the Bad Stuff Out of Where You Live (Your Inbox)

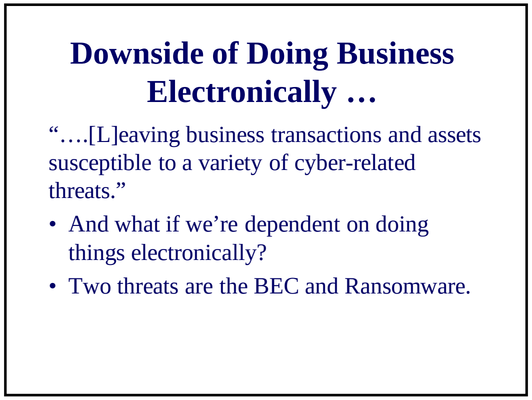


If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier

Benefits of Doing Business Electronically ….

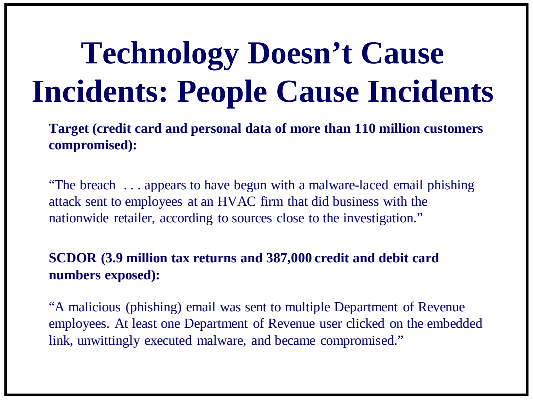
- It’s easy. It’s fast. It’s effective.
- Everybody’s doing it … "Virtually all economic activities now take place through digital technology and electronic communication ….”
- Your clients and customers EXPECT it …



Downside of Doing Business Electronically …

"….[L]eaving business transactions and assets susceptible to a variety of cyber-related threats."

- And what if we're dependent on doing things electronically?
- Two threats are the BEC and Ransomware.



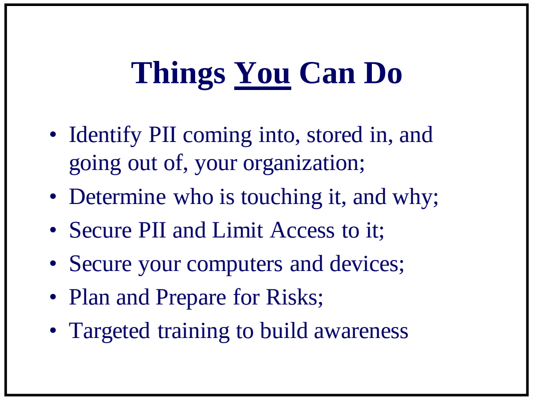
Technology Doesn't Cause Incidents: People Cause Incidents

Target (credit card and personal data of more than 110 million customers compromised):

"The breach . . . appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation."

SCDOR (3.9 million tax returns and 387,000 credit and debit card numbers exposed):

"A malicious (phishing) email was sent to multiple Department of Revenue employees. At least one Department of Revenue user clicked on the embedded link, unwittingly executed malware, and became compromised."



Things You Can Do

- Identify PII coming into, stored in, and going out of, your organization;
- Determine who is touching it, and why;
- Secure PII and Limit Access to it;
- Secure your computers and devices;
- Plan and Prepare for Risks;
- Targeted training to build awareness

Why is Awareness Important? Because Everybody Clicks

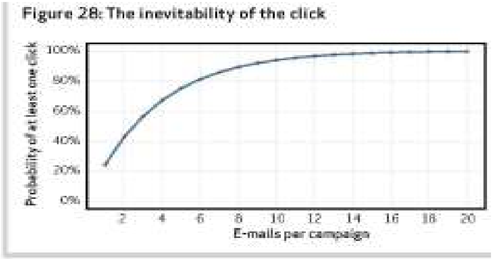
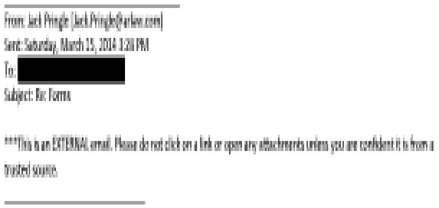


Figure 28: The inevitability of the click

Creating Awareness


From: Jack Pringle [Jack.Pringle@arlaw.com]
Sent: Saturday, March 15, 2014 3:28 PM
To: [redacted]
Subject: Re: Forms

***This is an EXTERNAL email. Please do not click on a link or open any attachments unless you are confident it is from a trusted source.

What is a BEC?

BEC is a scam attacking commercial, Government, and non-profit organizations that regularly perform wire transfer payments.

The email account compromise (EAC) part of BEC targets individuals who perform wire transfer payments.

What is Ransomware?

Malware that encrypts (locks up) files so you can't use them (and then demands a ransom).

[illegible].odin	[illegible] 10:10 AM	ODIN File	401 KB
[illegible].odin	[illegible] 10:13 AM	ODIN File	53 KB

How Does A Ransomware Attack Happen?

- Clicking on a malicious link in an email
- Opening an malicious attachment in an email

BEC on the Rise

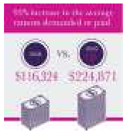
2017: IC3 received 15,690 BEC/EAC complaints with adjusted losses of over $675 million.

2018: IC3 received 20,373 BEC/EAC complaints with adjusted losses of over $1.2 billion.

29% increase in the number of complaints, and a **77% increase** in adjusted losses.

Source: 2017 and 2018 IC3 Internet Crime Reports

Ransomware on the Rise



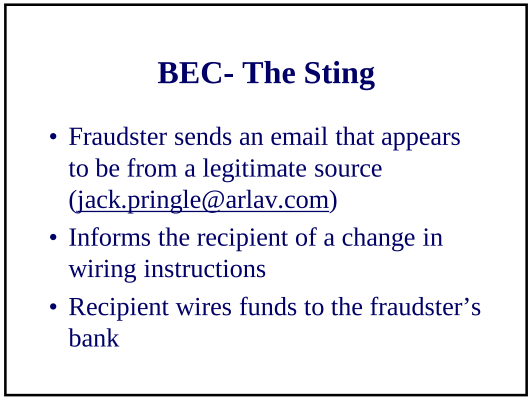
105% increase in the number of ransomware attacks
VS.

Ransomware Targets

Barracuda’s researchers conducted a deeper dive on 55 ransomware attacks on state, county and local governments that have taken place this year and found that 38 were on local governments, 14 were on county governments, and three were on state governments. *Nearly half of the government victims, around 45%, were small municipalities with populations of fewer than 50,000 residents, and 24% had fewer than 15,000 residents.*

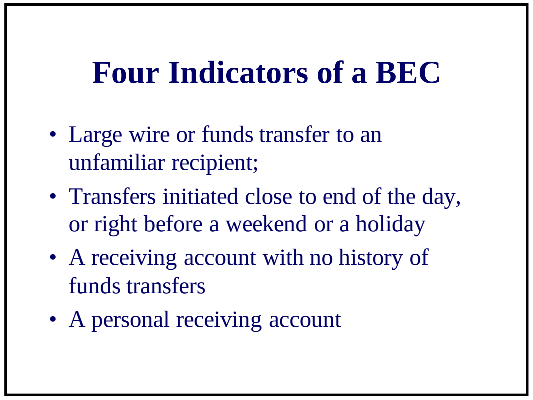
BEC – The Setup

- Bad actors get into the email system of a company
  - Malware
  - Social Engineering
- Spear Phishing-
  - Bad actors register “spoofed” domains and email accounts similar to the potential victim. (www.arlav.com).
  - The *From, Reply to,* and *Sender* fields look legitimate but are different.



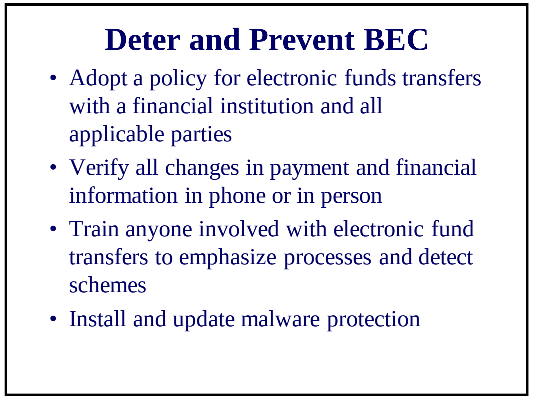
BEC- The Sting

- Fraudster sends an email that appears to be from a legitimate source (jack.pringle@arlav.com)
- Informs the recipient of a change in wiring instructions
- Recipient wires funds to the fraudster's bank



Four Indicators of a BEC

- Large wire or funds transfer to an unfamiliar recipient;
- Transfers initiated close to end of the day, or right before a weekend or a holiday
- A receiving account with no history of funds transfers
- A personal receiving account



Deter and Prevent BEC

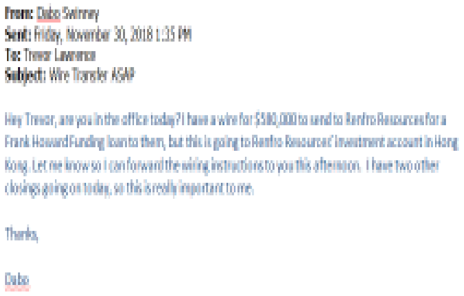
- Adopt a policy for electronic funds transfers with a financial institution and all applicable parties
- Verify all changes in payment and financial information in phone or in person
- Train anyone involved with electronic fund transfers to emphasize processes and detect schemes
- Install and update malware protection

Deter and Prevent BEC

- Conduct Daily Payment Activity Review
- Consider a dedicated computer for financial transactions

Report BEC Schemes

- Contact your financial institution and request a recall of funds
- Contact your local FBI office and report the fraudulent transfer. https://www.fbi.gov/contact-us/field-offices
- File a complaint with bec.ic3.gov.

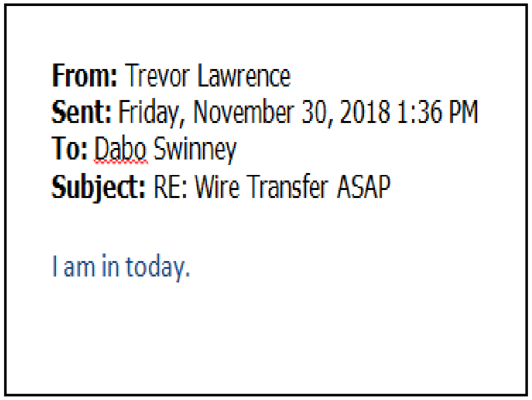


From: Dabo Swinney
Sent: Friday, November 30, 2018 1:35 PM
To: Trevor Lawrence
Subject: Wire Transfer ASAP

Hey Trevor, are you in the office today? I have a wire for $580,000 to send to Renfro Resources for a Frank Howard Funding loan to them, but this is going to Renfro Resources' Investment account in Hong Kong. Let me know so I can forward the wiring instructions to you this afternoon. I have two other closings going on today, so this is really important to me.

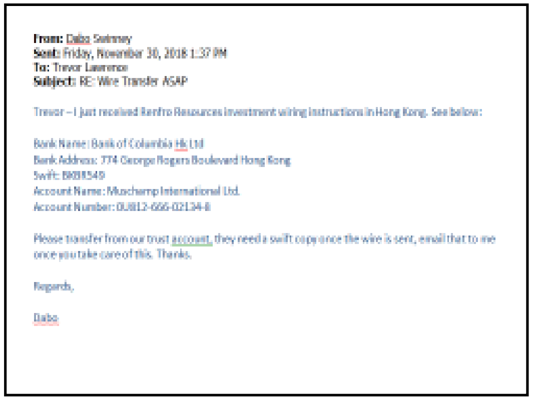
Thanks,

Dabo



From: Trevor Lawrence
Sent: Friday, November 30, 2018 1:36 PM
To: Dabo Swinney
Subject: RE: Wire Transfer ASAP

I am in today.



From: Dabo Swinney
Sent: Friday, November 30, 2018 1:37 PM
To: Trevor Lawrence
Subject: RE: Wire Transfer ASAP

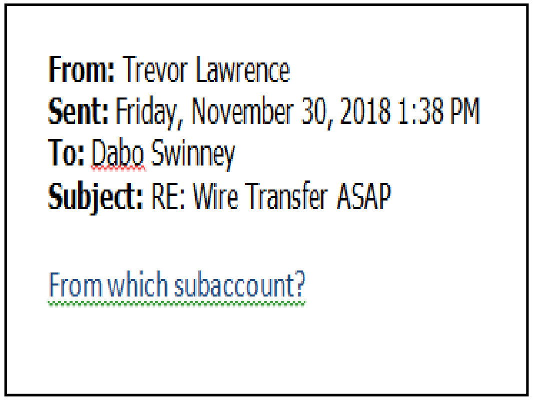
Trevor – I just received Renfro Resources investment wiring instructions in Hong Kong. See below:

Bank Name: Bank of Columbia Hk Ltd
Bank Address: 774 George Rogers Boulevard Hong Kong
Swift: BK88549
Account Name: Muschamp International Ltd.
Account Number: 0U812-666-02134-8

Please transfer from our trust account, they need a swift copy once the wire is sent, email that to me once you take care of this. Thanks.

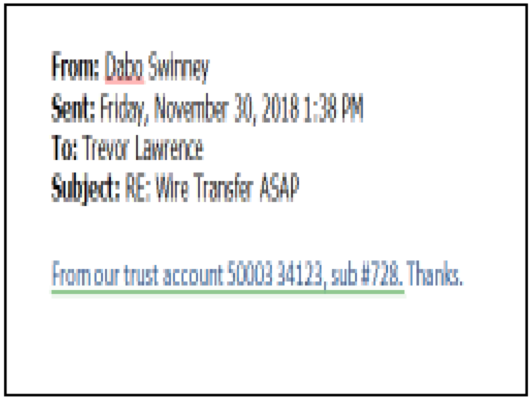
Regards,

Dabo



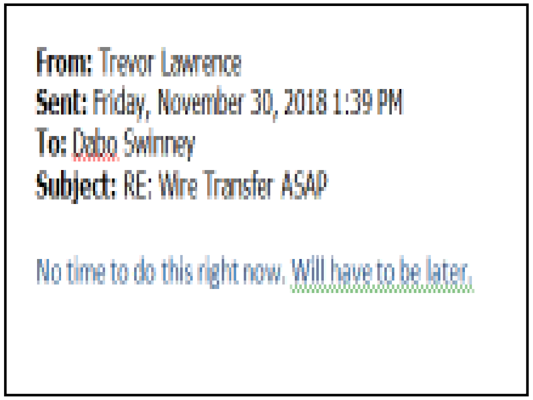
From: Trevor Lawrence
Sent: Friday, November 30, 2018 1:38 PM
To: Dabo Swinney
Subject: RE: Wire Transfer ASAP

From which subaccount?



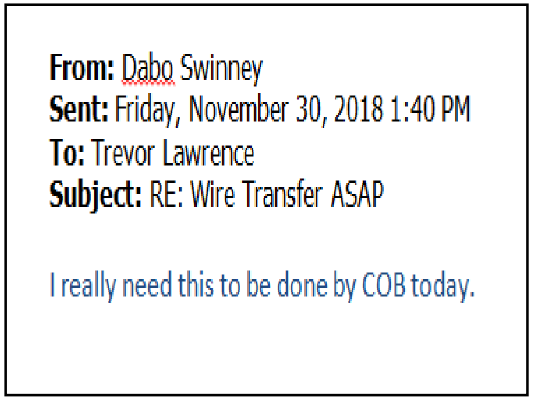
From: Dabo Swinney
Sent: Friday, November 30, 2018 1:38 PM
To: Trevor Lawrence
Subject: RE: Wire Transfer ASAP

From our trust account 50003 34123, sub #728. Thanks.



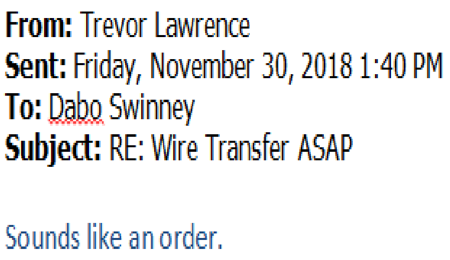
From: Trevor Lawrence
Sent: Friday, November 30, 2018 1:39 PM
To: Dabo Swinney
Subject: RE: Wire Transfer ASAP

No time to do this right now. Will have to be later.



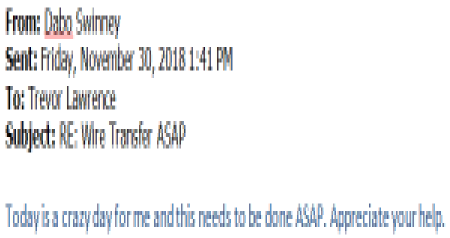
From: Dabo Swinney
Sent: Friday, November 30, 2018 1:40 PM
To: Trevor Lawrence
Subject: RE: Wire Transfer ASAP

I really need this to be done by COB today.



From: Trevor Lawrence
Sent: Friday, November 30, 2018 1:40 PM
To: Dabo Swinney
Subject: RE: Wire Transfer ASAP

Sounds like an order.

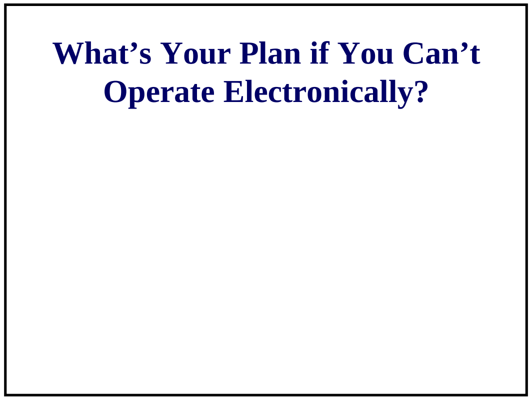


From: Dabo Swinney
Sent: Friday, November 30, 2018 1:41 PM
To: Trevor Lawrence
Subject: RE: Wire Transfer ASAP

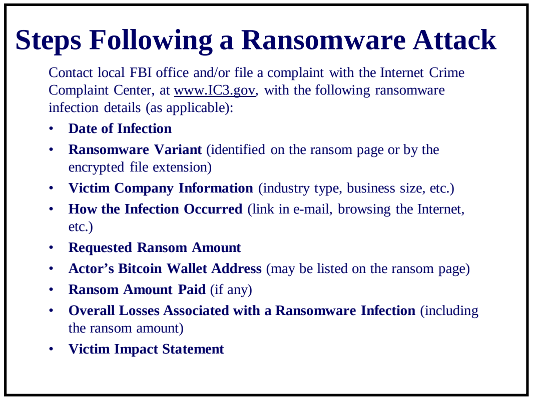
Today is a crazy day for me and this needs to be done ASAP. Appreciate your help.

Best Practices for Avoiding Ransomware Attacks

- Backup regularly and securely
- Be wary of links in and attachments to email messages
- Update and patch
- Employ and update anti-malware tools
- Don’t store documents locally



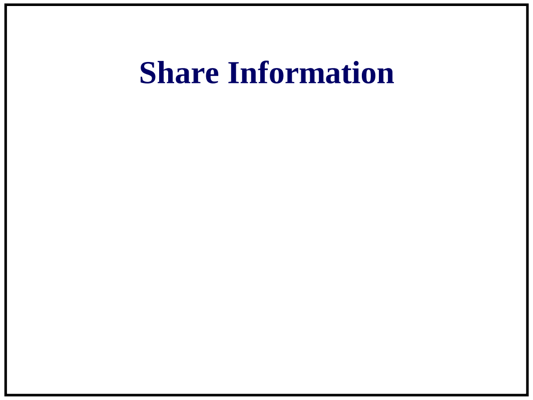
What’s Your Plan if You Can’t Operate Electronically?



Steps Following a Ransomware Attack

Contact local FBI office and/or file a complaint with the Internet Crime Complaint Center, at www.IC3.gov, with the following ransomware infection details (as applicable):

- **Date of Infection**
- **Ransomware Variant** (identified on the ransom page or by the encrypted file extension)
- **Victim Company Information** (industry type, business size, etc.)
- **How the Infection Occurred** (link in e-mail, browsing the Internet, etc.)
- **Requested Ransom Amount**
- **Actor’s Bitcoin Wallet Address** (may be listed on the ransom page)
- **Ransom Amount Paid** (if any)
- **Overall Losses Associated with a Ransomware Infection** (including the ransom amount)
- **Victim Impact Statement**

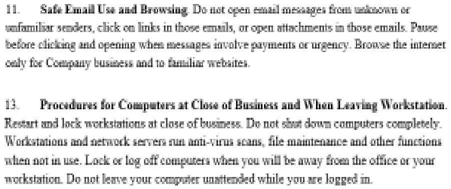


Share Information

Strengthen Your Security Program

- Conduct **targeted** training based on risks.
- Patch regularly and systematically.
- Implement least access privilege.
- Categorize information and segment it.

Do Your Policies Address These Threats?



11. **Safe Email Use and Browsing**. Do not open email messages from unknown or unfamiliar senders, click on links in those emails, or open attachments in those emails. Pause before clicking and opening when messages involve payments or urgency. Browse the internet only for Company business and to familiar websites.

13. **Procedures for Computers at Close of Business and When Leaving Workstation.** Restart and lock workstations at close of business. Do not shut down computers completely. Workstations and network servers run anti-virus scans, file maintenance and other functions when not in use. Lock or log off computers when you will be away from the office or your workstation. Do not leave your computer unattended while you are logged in.

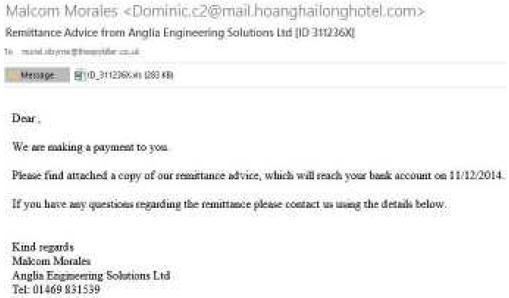
Tips

- ***Don't Click*** on attachments and links in emails from senders you don't recognize
- ***Verify*** (on the phone) instructions from senders you THINK you recognize BEFORE YOU CLICK
- ***Don't store*** critical data on your desktop
- **Don't let distraction and "urgency" overcome your patience and skepticism.**

Don’t Fall for the “Urgent”

- If you get an email that looks legitimate, log in to your account separately (WITHOUT CLICKING IN AN EMAIL)
- If you get “wire transfer” requests or notices via email, *call* the sender to confirm.

Don’t Get Excited About Getting Paid



Malcom Morales <Dominic.c2@mail.hoanghailonghotel.com>

Remittance Advice from Anglia Engineering Solutions Ltd [ID 311236X]

To [illegible]

Dear ,

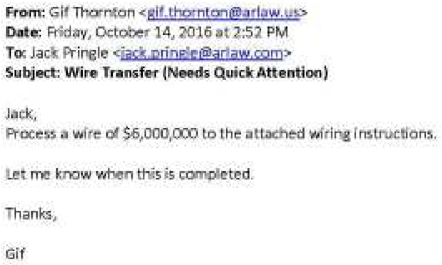
We are making a payment to you.

Please find attached a copy of our remittance advice, which will reach your bank account on 11/12/2014.

If you have any questions regarding the remittance please contact us using the details below.

Kind regards
Malcom Morales
Anglia Engineering Solutions Ltd
Tel: 01469 831539

Verify Authority



From: Gif Thornton <gif.thornton@arlaw.us>
Date: Friday, October 14, 2016 at 2:52 PM
To: Jack Pringle <jack.pringle@arlaw.com>
Subject: Wire Transfer (Needs Quick Attention)

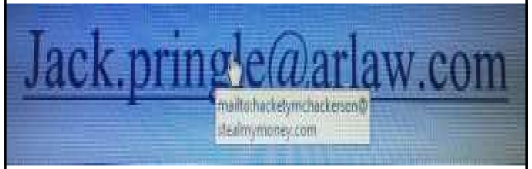
Jack,
Process a wire of $6,000,000 to the attached wiring instructions.

Let me know when this is completed.

Thanks,

Gif

Hover (Without Clicking)



Jack.pringle@arlaw.com

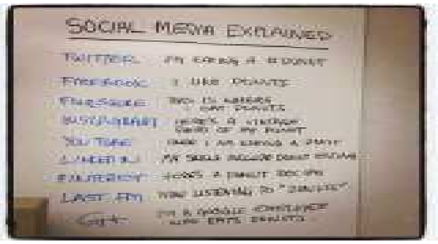
mailto:hacketymchackerson@
stealmymoney.com

Don’t Save Documents Locally (Unless You Want to Lose Them)

Takeways

- **Don’t Click** on attachments and links in emails from senders you don’t recognize;
- **Verify** (in person or on the phone) messages from people you THINK you know BEFORE YOU CLICK;
- Pause and don’t get conned.
- Don’t store documents on your work station

Social Media



SOCIAL MEDIA EXPLAINED

TWITTER	I'M EATING A #DONUT
FACEBOOK	I LIKE DONUTS
FOURSQUARE	THIS IS WHERE I EAT DONUTS
INSTAGRAM	HERE'S A VINTAGE PHOTO OF MY DONUT
YOU TUBE	HERE I AM EATING A DONUT
LINKEDIN	MY SKILLS INCLUDE DONUT EATING
PINTEREST	HERE'S A DONUT RECIPE
LAST FM	NOW LISTENING TO "DONUTS"
G+	I'M A GOOGLE EMPLOYEE WHO EATS DONUTS

Gaps Between Employers and Employees

- Expectations, Worldview
- The Lines Between Personal and Business are Being Blurred

Importance of Policies

"employer policies concerning communication will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

City of Ontario v. Quon, 130 S.Ct. 2619 (2010).

Questions?

Jack Pringle
Adams and Reese LLP
(803) 343-1270
jack.pringle@arlaw.com
Twitter: @jjpringlesc
www.linkedin.com/in/jack-pringle-5834554
www.slideshare.net/jjpringle317

References

SEC Report of Cyber-Related Frauds, SECURITIES EXCHANGE ACT OF 1934 Release No. 84429 / October 16, 2018 https://www.sec.gov/litigation/investreport/34-84429.pdf

"Ransomware Victims Urged to Report Infections to Federal Law Enforcement," FBI Public Service Announcement, Alert No. I-091516-PSA, September 15, 2016 https://www.ic3.gov/media/2016/160915.aspx

"Business E-Mail Compromise: The 12 Billion Dollar Scam," FBI Public Service Announcement, Alert No. I-071218-PSA, July 12, 2018, https://www.ic3.gov/media/2018/180712.aspx

"Regional municipal ransomware attacks soar; MS-ISAC can help," CSO, August 28, 2019, https://www.csoonline.com/article/3433930/regional-municipal-ransomware-attacks-soar-ms-isac-can-help.html

MS-ISAC, Multi-State Information Sharing and Analysis Center, https://www.cisecurity.org/ms-isac/

"Ransomware Attacks Skyrocket, Q1 2019," Beazley Breach Insights, May 23, 2019 https://www.beazley.com/news/2019/beazley_breach_insights_may_2019.html

"Best Practices for Victim Response and Reporting of Cyber Incidents," U.S. Department of Justice, Version 1.0 (April 2015).
https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf

2017 Internet Crime Report, FBI Internet Crime Center (IC3), issued May 7, 2018, https://pdf.ic3.gov/2017_IC3Report.pdf

2018 Internet Crime Report, FBI IC3, issued April 22, 2019, https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf