



Stealing Home... Depot f/k/a **Don't** Be a Target!



Post-Mortem of the latest data breaches, with tips to help you avoid becoming the next Target, Kmart, Dairy Queen, Home Depot.



Don't Be a Target!

Eric Selje

Madison, WI

@EricSelje

Salty Dog Solutions, LLC

Database Developer

General IT Guy









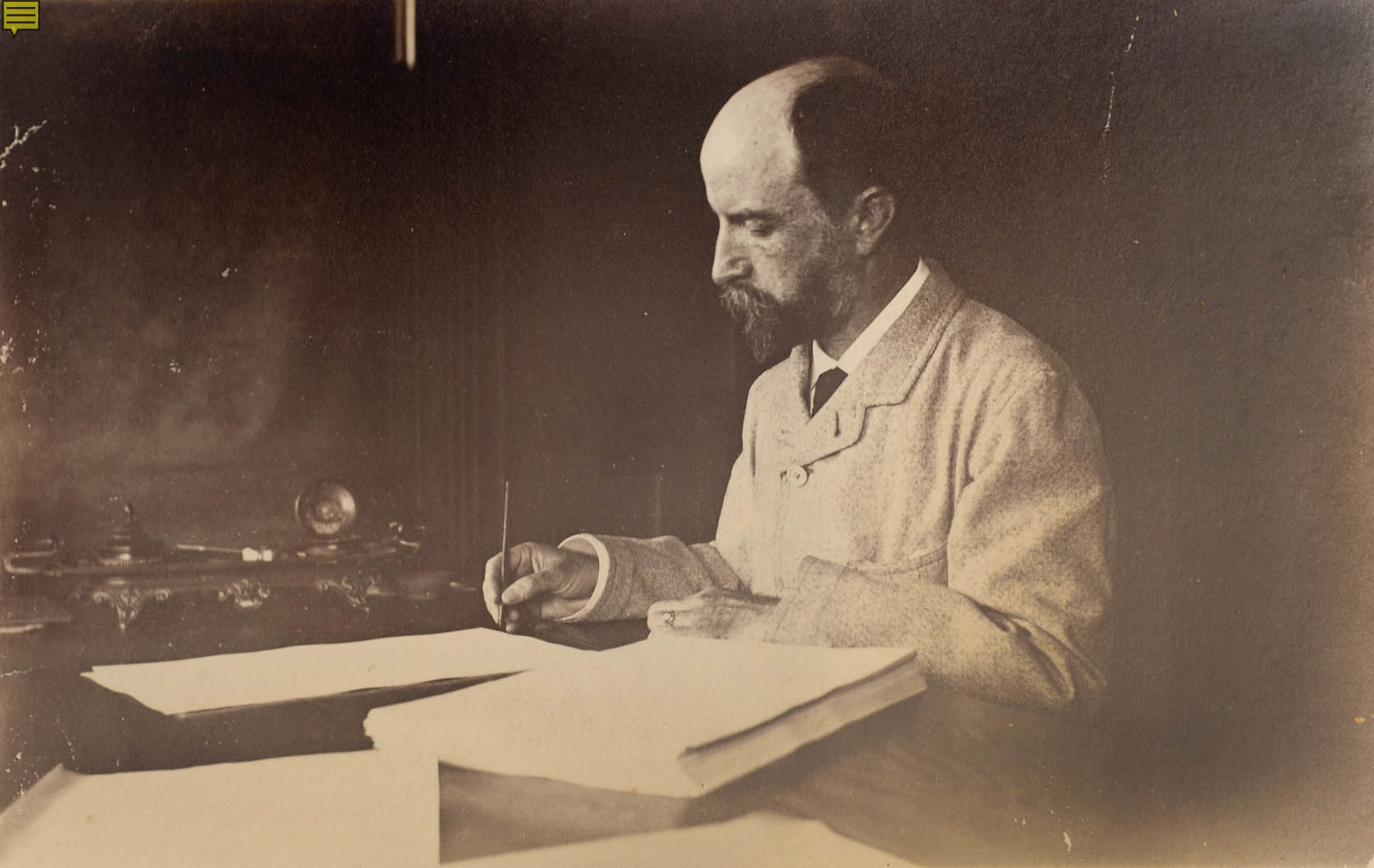


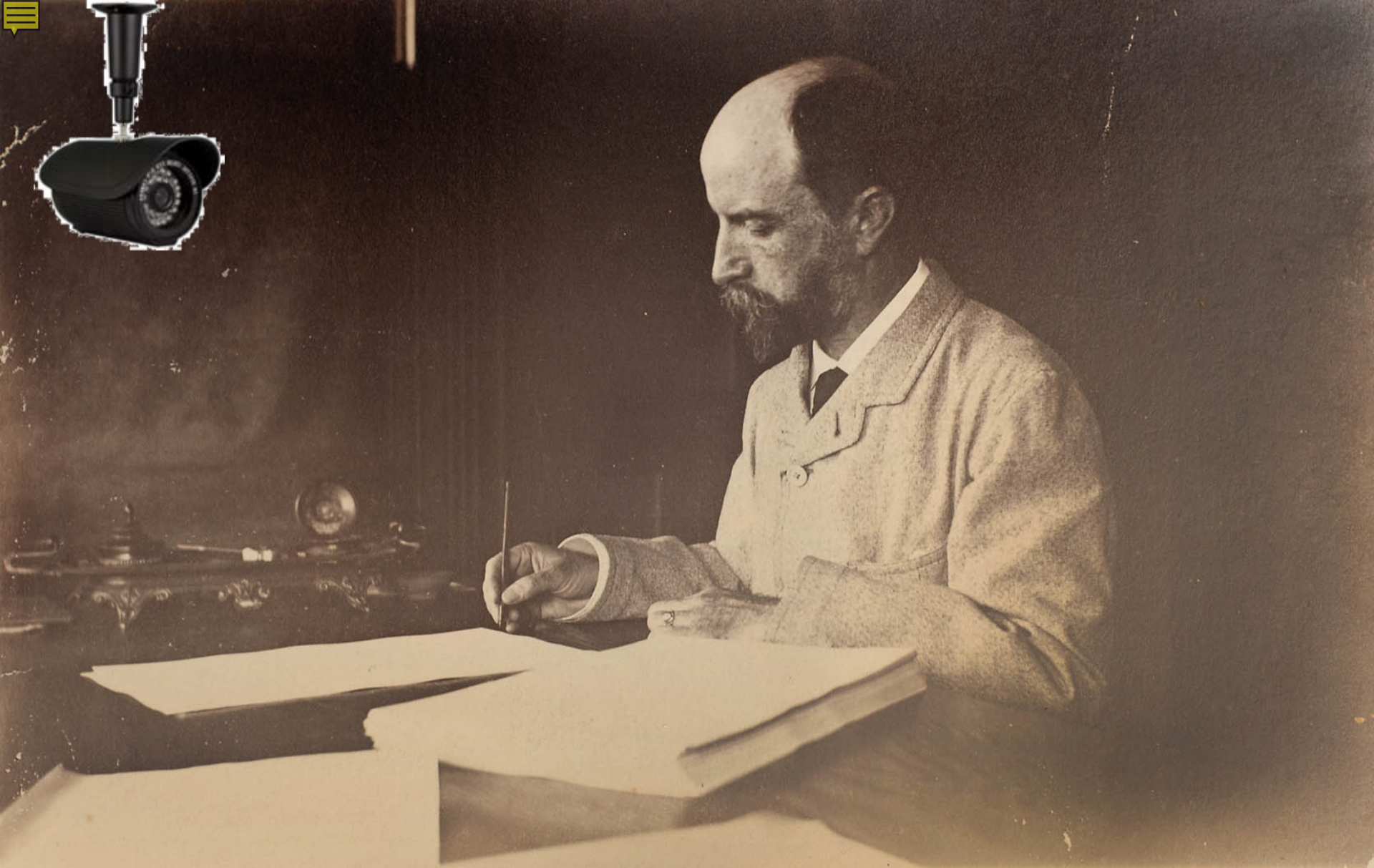


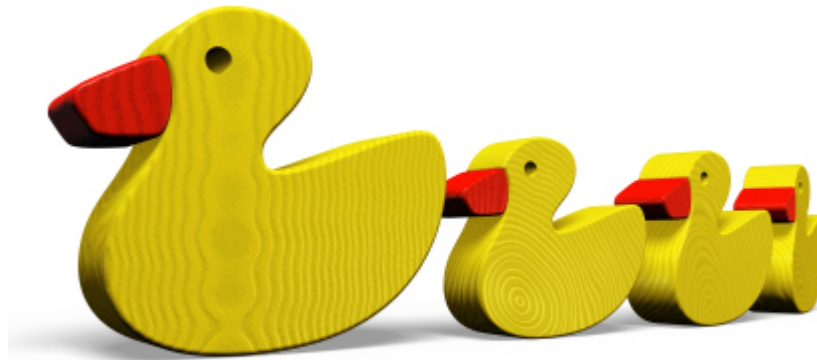


“RAM Scraping”











Fazio Mechanical Services

Fazio Mechanical is "Refrigeration"



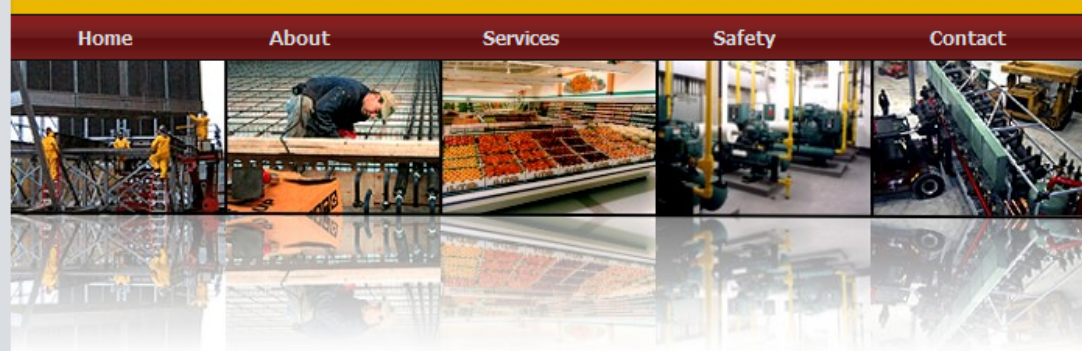
- About Fazio Mechanical
- Fazio Services
- Safety Dedicated
- Directions to Fazio
- Contact Fazio

412-782-6338

800-241-4029

Fazio Mechanical is licensed in:

- Pennsylvania
- West Virginia
- Maryland
- Virginia
- Ohio

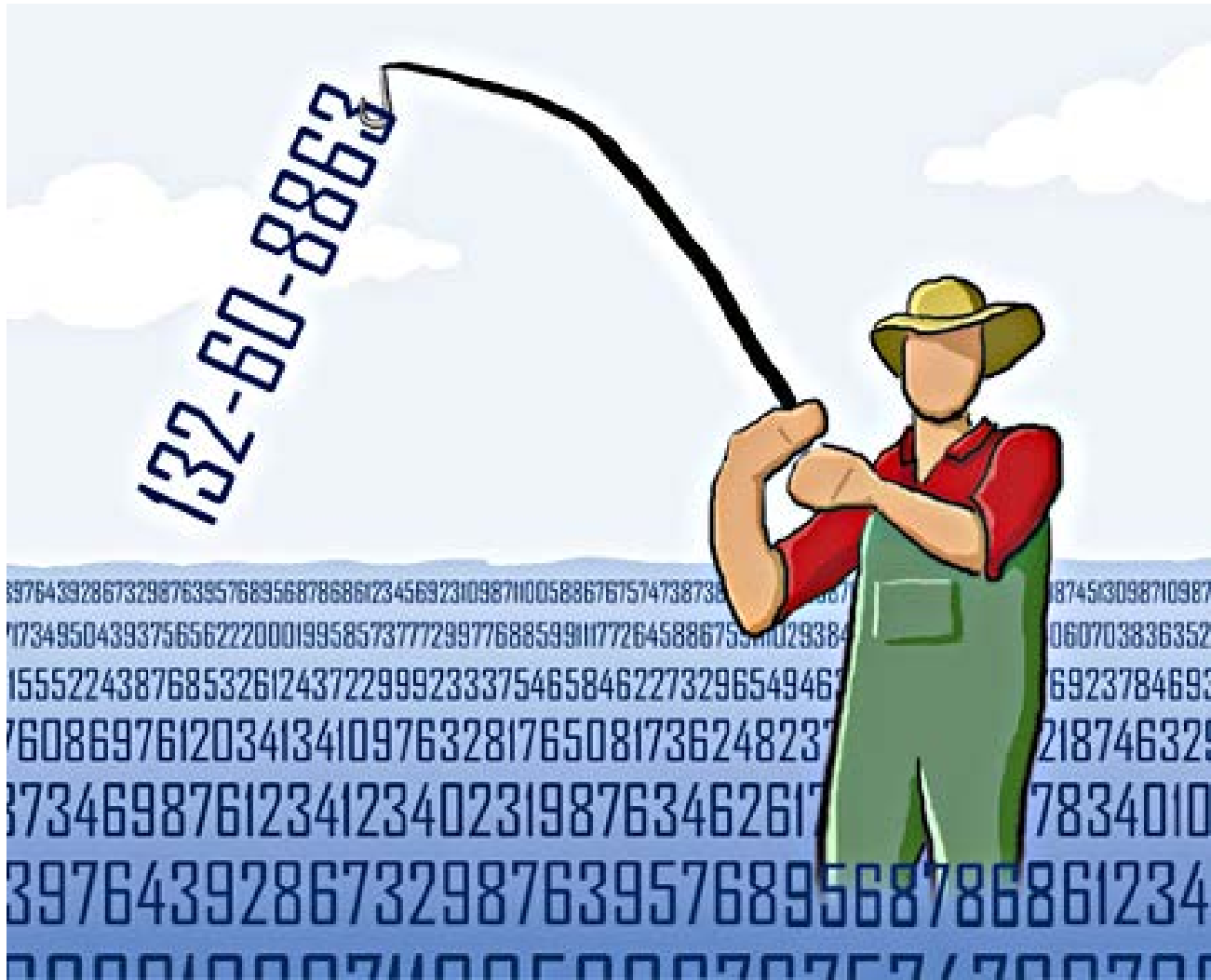


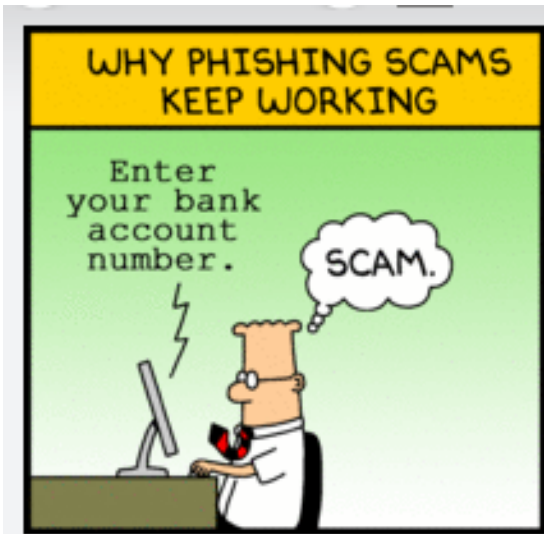
At Fazio Mechanical we have a passion for design, engineering, installation, service and support and all while keeping a focus on saving energy. [Learn more ...](#)

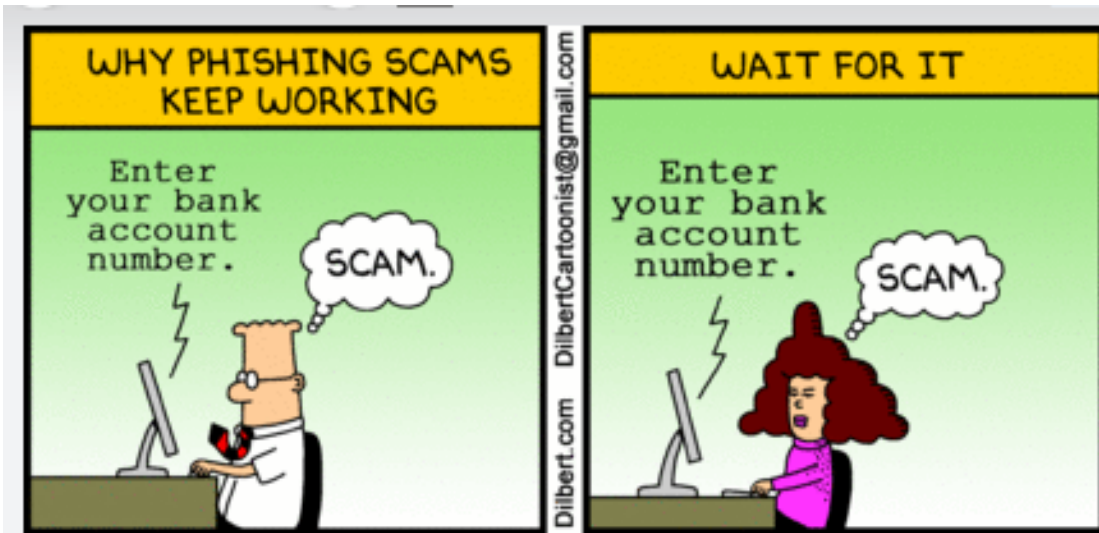
Fazio Mechanical Services is a full-service mechanical contractor that specializes in the design, installation, and service of the most advanced, cost effective and environmentally-friendly supermarket refrigeration systems in the industry.

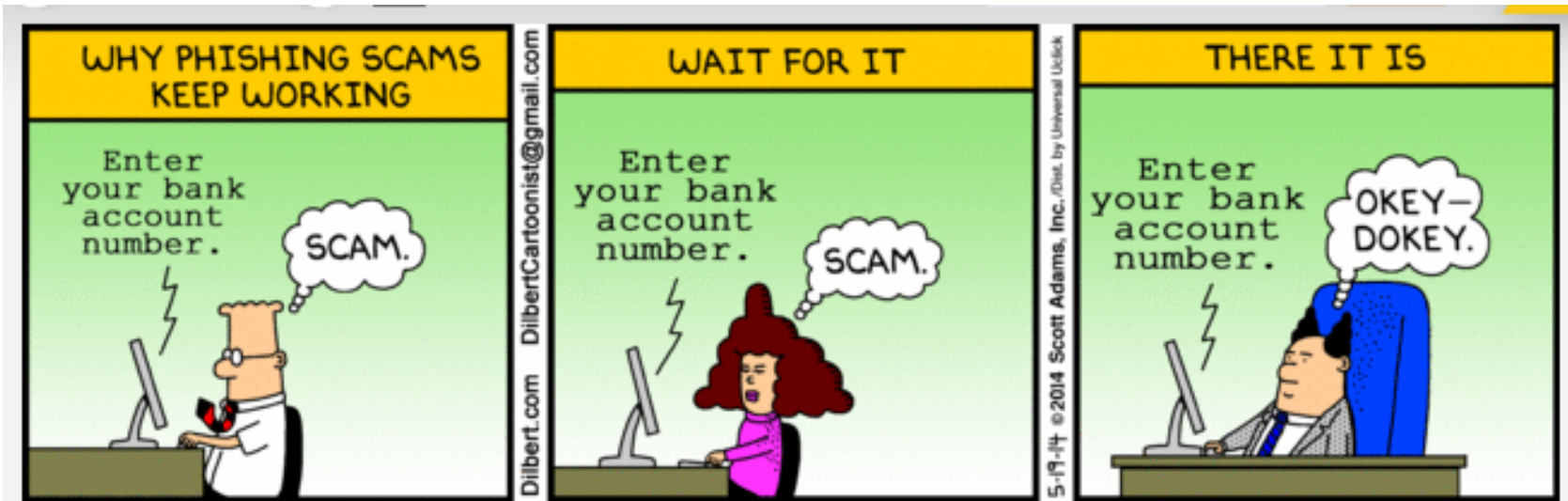
We service customers in Western Pennsylvania, Eastern Ohio, and parts of West Virginia, Maryland and Virginia. We bring the technical knowledge, experience, and proven performance that is "second-to-none" in the refrigeration industry.

"Fazio Mechanical is Refrigeration"











Lesson: Know your Scams

- *And share what you know with everybody, including your pointy-haired boss.*



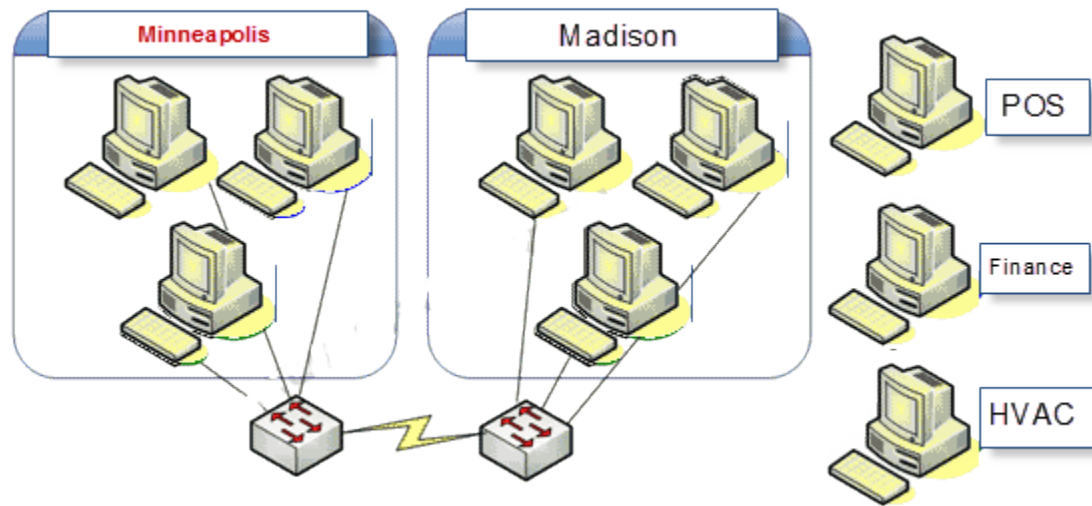


Lesson: Don't be a Fazio!

- *You are only as secure as your subcontractors and or third-party vendors, and your clients are only as secure as you are!*

*If you're a consultant/subcontractor/vendor,
Don't be a Fazio.*

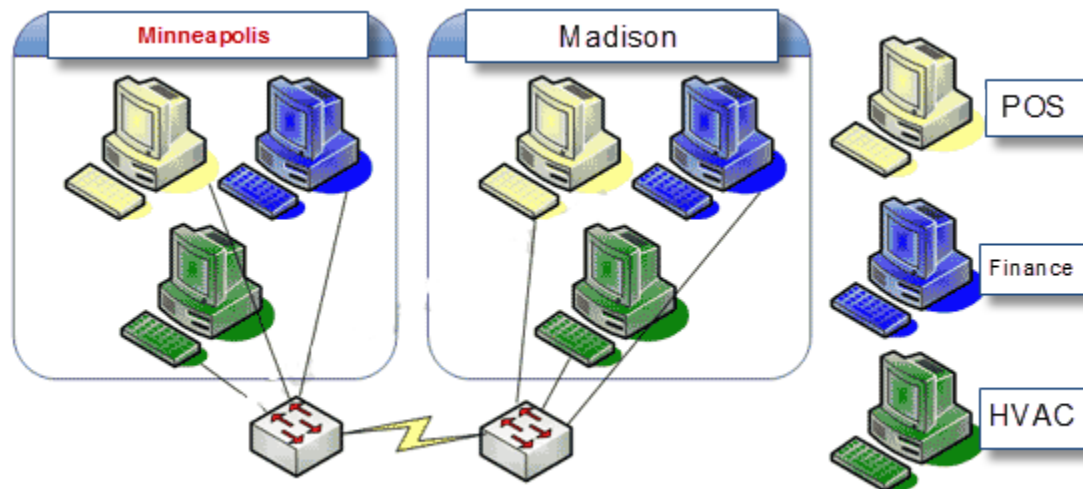
Keep yourself covered.

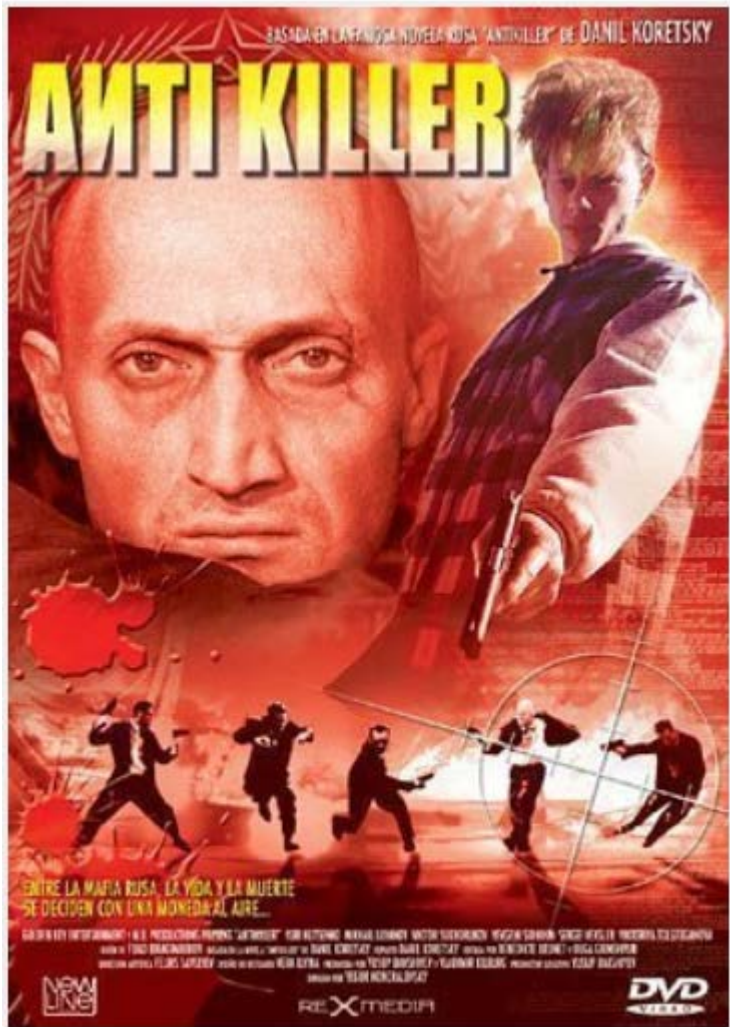


Lesson: Don't Cross the Streams



Lesson: Segment Your Network





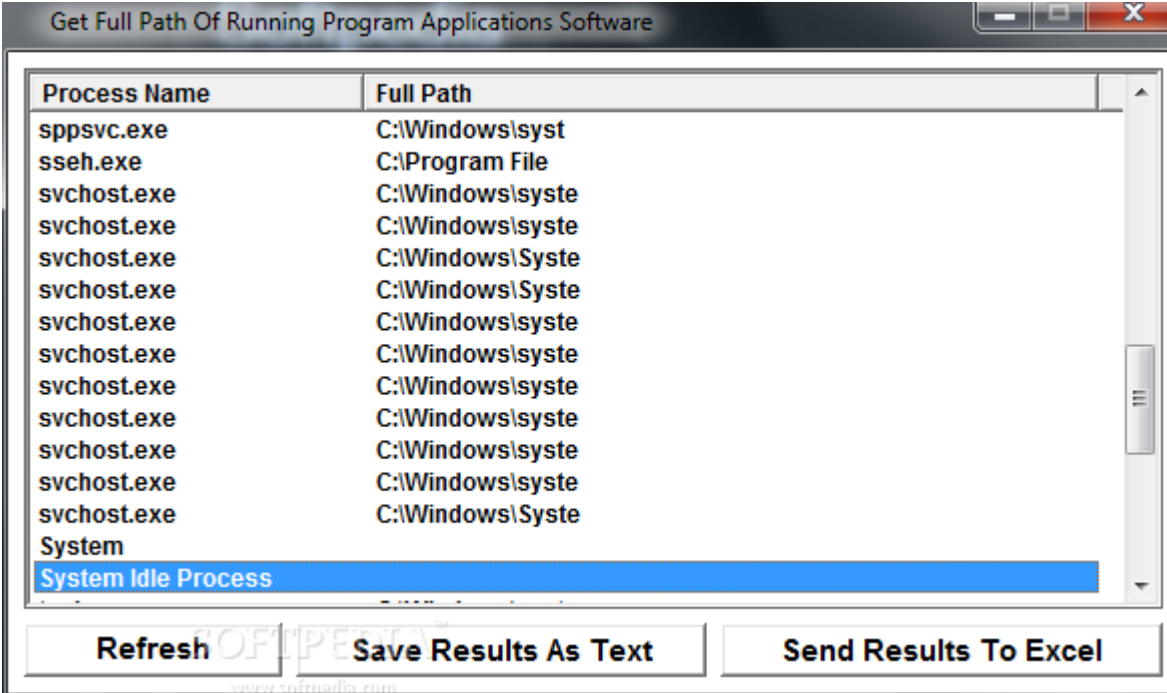




BLACK
FRIDAY

Lesson:

Know What's Running on Your Servers



Process Name	Full Path
sppsvc.exe	C:\Windows\sys
sseh.exe	C:\Program File
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\Syste
svchost.exe	C:\Windows\Syste
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
svchost.exe	C:\Windows\sys
System	
System Idle Process	





November 2013

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

© www.calendarpedia.com

Dates provided 'as is' without warranty









Krebs on Security

In-depth security news and investigation



Coming Soon

<http://rescator.so>

[Register](#)

Login

Login: *

Password: *

Code: ~~2 1 3 4 0~~

[Refresh](#)

*

Login

WARNING

Support:

 [Read before contacting us on ICQ.](#)

 17700

 10576

Warning!

[Register](#)

Login

Warning

Rescator.SO - Rescator.CO - Rescator.CC - Rescator.CM
Octavian.SU - Octavian.SO - Octavian.CM

The only official & genuine shop links. [All others are clone rippers!](#)

List of known clone **ripper sites** demanding activation fee to register:

rescator.su	jshop.su
reskator.la	lampeduza.su
approved1.ru	feshop.su
uniccshop.su	backstab.su
crdsu.net	bstab.biz
maza.su	cvv2shop.ru
ccvalid.su	swiped.su
ccbases.su	secretshop.su
sruka.su	

These sites are not affiliated with us in any way and copied only to scam your money. Beware and let us know of any additional sites you may approach.



<http://rescator.su>

[Register](#) [Login](#)

Login

Login: *

Password: *

Login

Support:

JID: trayan@lampeduza.org

ICQ: 100845

JID 2: flavius@lampeduza.org


ICQ 2: 17700

JID 3: rescator@lampeduza.org

ICQ 3: 10576

Первый кардинг форум





WALLET	CART
\$0.00	0
<small>add funds</small>	<small>view items</small>

BROWSE DUMPS

- WHOLESALE**
- ACCOUNT
- CHECKER
- SUPPORT

Wholesale

* Dumps from packs are not refundable

1245

for \$10,500.00

Reseller	McDumpals
Base	MA-CT
Date pre-sale	2014-03-31
Date sale	2014-03-31
Age	1 month and 10 days
Details	View more

asd

Quick buy

Add to cart

1110

for \$7,500.00

Reseller	McDumpals
Base	MA-CT
Date pre-sale	2014-03-31
Date sale	2014-03-31
Age	1 month and 2 days
Details	View more

Buyme!


Quick buy

Add to cart

x

35 | 3/29/14|

© Eric Selje

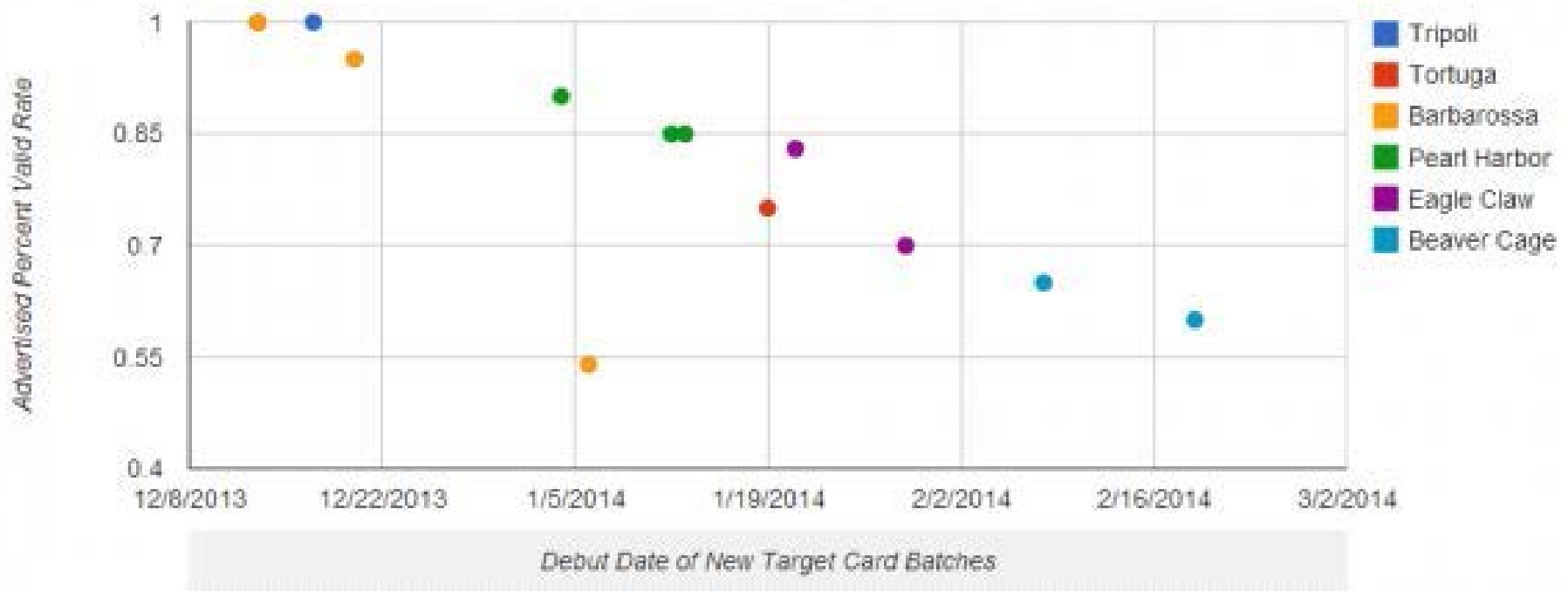


PASS SQL Saturday

#287 | MADISON 2014



Valid Rate Decline for Cards Stolen in Target Breach





[EVEN MORE USA DUMPS UPDATED](#) / [07 SEPTEMBER 2014](#) / [COMMENTS](#):

Even more USA Dumps updated!

Base name: **American Sanctions 6, 7, 8, 9**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 10, 11, 12**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

[USA DUMPS UPDATE!](#) / [04 SEPTEMBER 2014](#) / [COMMENTS](#):

USA Dumps update you asked for!

Base name: **American Sanctions 5**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: **American Sanctions 4**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

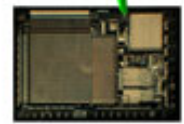
Base name: **American Sanctions 3**
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!



MicroChip

Security Keys
Card Holder Data

Software



Brand Marks,
Hologram,
Magnetic Stripes..

Plastic Card Body

Personalization,
Embossing,

CAV2/CID/CVC2/CVV2
(all other payment brands)



Magnetic stripe
(data on tracks 1 & 2)







VISA



DISCOVER
NETWORK

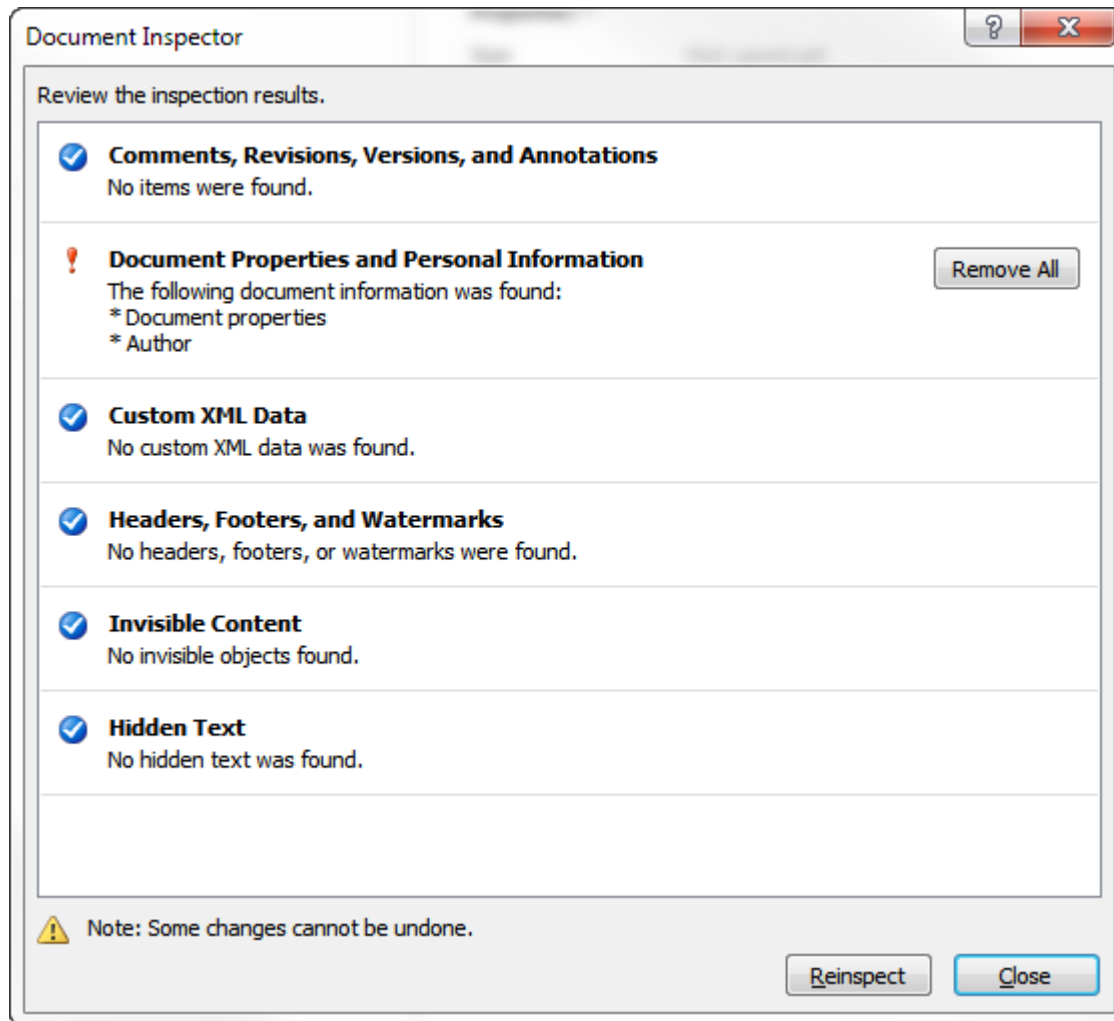


citibank

Bank of America



Capital One







Summary (Lessons Learned)

- Don't be a Fazio!
Make sure you and your vendors are secure
- Keep abreast of the latest scams (and share!)
- Least Privilege Principle
- Segment Your Network (Don't Cross the Streams)
- Know What's Running on Your Servers
- Separate Signal from Noise, and pay attention to the signals



Resources

- <http://www.jupiterbroadcasting.com/51107/targeting-the-hvac-techsnap-148/>
- @allanjude
- @chrisLAS
- <https://www.cs.columbia.edu/~smb/blog/2014-02/2014-02-05.html>
- <http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>
- <http://www.infrasupport.com/target-get-on-the-ball-with-this-data-breach/>
- <http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690>
- <http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/An-evolution-of-BlackPOS-malware/ba-p/6359149#.Uy9FvFeo11k>
- <http://www.informationweek.com/security/attacks-and-breaches/target-breach-8-facts-on-memory-scraping-malware/d/d-id/1113440>
- <http://security.stackexchange.com/questions/46319/why-emv-cards-cannot-be-cloned>
- <http://www.npr.org/blogs/alltechconsidered/2014/01/23/264910138/target-hack-a-tipping-point-in-moving-away-from-magnetic-stripes>
- <http://www.xylibox.com/2012/03/pos-carding.html>
- <http://www.slideshare.net/AlertLogic/the-target-breach-anatomy-of-an-attack>
- Photograph of Henry Adams writing at desk by Marian Hooper Adams (1843–1885) (Massachusetts Historical Society) [Public domain], via Wikimedia Commons