You’ve Been Hacked - Now What?
10 Tips for Effective Response
@regharnish
Lahore, Pakistan – February 2011
Searching for “Brain” – the first computer virus
HOW DID WE GET HERE?
COMPLEXITY
Gone Phishin’
From: noreply@direct.nacha.org <loonierm37@immediaconsulting.com>
To: Reg Harnish
Cc: 
Subject: Direct Deposit payment ID 418268376701 rejected

Hereewith we are informing you, that your latest Direct Deposit payment (#753806224605) was declined, because of your current Direct Deposit software being out of date. Please visit the secure section of our web site http://cregybad.org/track.php?c003

Details

Please refer to your financial institution to obtain the updated version of the software.

Sincerely yours

ACH Network Rules Department
NACHA | The Electronic Payments Association

15947 Sunrise Valley Drive, Suite 884
Herndon, VA 27212
Phone: 703-454-0961 Fax: 703-775-4918
Dear valued customer,

To get back into your PayPal account, you'll need to update your account information.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.
4. Click to follow link

Link Now
fish
rharnish@greycastlesecurity.com,

Amber Larson, wants to connect with you on LinkedIn.

Amber Larson,
Financial Services Professional
http://50.63.46.110/dreadful/index.html
Click to follow link

You are receiving invitation emails. Unsubscribe

This email was intended for rharnish@greycastlesecurity.com Learn why we included this. © 2013, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

See more about: Della Gordon.
Gone Phishin'
YOU’VE BEEN

NOW WHAT?

HACKED
1. Learn how to:

Perform Triage

- Secure the crime scene
- Establish communications channels
- Assess size, scope and severity
- Manage expectations
2. Build your: Incident Response Team

- Find the best responders – they are unique
- Train responders on the right things
- Include representatives from the business
- Outsource expertise that is not a core competency
3. Learn how to:

Perform Forensics

• Decide ASAP if you’re going to litigate
• Allow your attorney to drive the investigation
• Establish chain of custody
• Log everything
4. Make sure to:

Manage IT Staff

- Keep IT staff from overstepping their capabilities
- Maintain contacts lists for law enforcement, digital forensics experts and attorneys
5. Learn how to:

Conduct Investigations

- Know what’s worth stealing
- Identify Indicators of Compromise (IoC)
- Preserve evidence correctly
6. Configure assets to:

Generate Intelligence

- Log events that may be needed for response
- Understand what “normal” is
7. Learn how to:

Report Breaches

- Understand your reporting requirements
- Maintain notification templates
- Allow attorney to define “reasonable”
8. Get to:

Love Your Attorney

- Prepare to be sued by customers, partners, banks
- Engage an attorney early for privilege
- Allow legal team to drive data retention
- Sic attorney on cloud, hosting and other providers
9. Make sure to:

Test and Train

- Test your Incident Response Plan
- Train teams on your Incident Response Plan
- Measure response capability
- Budget for testing and training
10. Consider:

Get Insured

- Minimize policy premiums by managing risk
- Understand the fine print
- Prepare for a battle
INCIDENT RESPONSE

STANDARDS
Standards

- NIST Computer Security Incident Handling Guide
  

  

- ENISA Incident Handling Process
  
Breach Reporting

- HIPAA HITECH Breach Notification Rule
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
- FTC Safeguards Rule
FINAL THOUGHTS
Know the difference between EXPOSURE AND A BREACH.
Know when to **CUT YOUR LOSSES.**
Learn how to SURVIVE.
Life as a Business Associate (BA)

- Life changed in 2013 and 2014 with the implementation of HiTECH and HHS’s Risk Assessment tool.

- The realization of HIPAA’s requirements has been slow in the Behavioral Health world as it hasn’t been the focus of enforcement.

- BAs are now treated as though they are Covered Entities and Covered Entities can no longer use “not knowing” as a defense against a breach.

- There is some question as to how much investigating you, as Covered Entities, ought to do on your BAs, but certainly, asking if they are HIPAA compliant isn’t enough. Ideally, they have a 3rd party Risk Assessment they can summarize for you.
FOOTHOLD’S STATUS

- Foothold Technology’s security is second to none.
- Claims of 100% compliance should be viewed skeptically.
- Physical, Administrative and Technical safeguards can reach deep in to a company’s operations and way out to their clients’ operations.
- AlertLogic for 24/7 monitoring of threats, vulnerabilities, and user logging, Workspaces (no ePHI on workstations), Active Directory (encryption), etc.
GOT QUESTIONS?