

Technology Security

Presenter(s)

Heather Helm, NMDP Product Owner, Donor Services

Rob Hanson, NMDP Cyber Security and Privacy Director

Disclosures

The following faculty and planning committee staff have no financial disclosures:

Name	Institution
Heather Helm	NMDP/Be The Match
Rob Hanson	NMDP/Be The Match
Brandon Knez	NMDP/Be The Match
Lara Rauchwarter	NMDP/Be The Match

Disclosures

The following faculty and planning committee staff have the following financial disclosures:

Name	Institution	Disclosure
Jackie Foster, MPH, RN, OCN	NMDP/Be The Match	Pfizer, stock ownership (spouse)

Learning objectives

At the conclusion of this session, attendees will be able to:

- Examine the different types of cyber-criminals that are targeting healthcare and their motives for stealing and monetizing healthcare data.
- Explore why healthcare staff, not the technology, are the primary target of these cyber-attacks.
- Apply basic techniques to foil cyber-attacks in your daily workplace.

Cyber Risk Climate Change

- ↑ Monetization of medical records
- ↑ Attack methods (ransomware), sophistication
- ↑ Disruptive technologies (social, mobile, analytics, cloud)
- ↑ Accountability and regulatory changes (General Data Protection Regulation)
- ↑ Health sector breaches
- ↑ Business impact and consequences (breach costs, sanctions)





The success of our shared mission depends on managing cyber risks across a connected healthcare ecosystem and interconnected networks.

Hacking Economics: Medical Records

Because of the unique information in medical records, hackers can offer more valuable products to clients.


1. Higher black market sales prices (compared to financial or retail records)
2. Procurement of pharmaceutical drugs
3. Medical insurance fraud
4. Tax fraud
5. “Fullz” to replace a complete identity, credentials (e.g., Passports)
6. Medical applications are critical for patient care - ripe for extortion (ransomware)
7. Healthcare is a soft target

Hacking Economics: Medical Records



Medical Fullz

PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisitType,NextApptDate,NextVisitType,LastDOS,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,First,Last,Title,LastPract,LastBase,LastTotal
NO Refund.

Sold by  - 3 sold since Jul 7, 2016 **Vendor Level 5** **Trust Level 5**

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / Item

Purchase price: USD 5.00

Qty: **Buy Now** **Queue**

0.0083 BTC / 0.5176 XMR

[Description](#) [Bids](#) [Feedback](#) [Refund Policy](#)


Product Description

PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisitType,NextApptDate,NextVisitType,LastDOS,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,First,Last,Title,LastPract,LastBase,LastTotal

NO Refund.


[Doctor](#) [health](#) [medical](#)

Hacking Economics: Medical Records



EXCLUSIVE FARMED IDENTITY a new Identity for a new life - 100% positive feedback - 100% satisfaction guaranteed

(this is the \$1000 deposit listing, it's FE, use it to start the process and submit your criteria. This value will go towards your final price obviously - the remaining balance will be in ESCROW) CRITERIA NEEDED: Acceptable age range Acceptable height or range of heights acceptable eye color(s) Race/Ethnicity Sex OPTIONAL CRITERIA: Hair color Acceptable Weight range Intended usag...

Sold by  - 304 sold since Apr 5, 2015 **Vendor Level 6** **Trust Level 6**

	Features		Features
Product class	Digital goods	Origin country	United States
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,000.00

Qty: 1 **Buy Now** **Queue**

1.8532 BTC / 102.8866 XMR

[Description](#) [Bids](#) [Feedback](#) [Refund Policy](#)

Product Description

(this is the \$1000 deposit listing, it's FE, use it to start the process and submit your criteria. This value will go towards your final price obviously - the remaining balance will be in ESCROW)

CRITERIA NEEDED:
Acceptable age range
Acceptable height or range of heights
acceptable eye color(s)
Race/Ethnicity
Sex

Hacking Economics: Medical Records

...onion All products My purchases Messages Account (0.0 BTC) Log out

You don't have enough funds for this product. Start by loading balance to **your account**.

400 Pills Ambien (Generic) 10 MG

488.48 EUR (0.885761 BTC)
more than 25 pcs in stock
(542 / -4)
United States → Worldwide

1 Buy

Ambien (zolpidem) is a sedative, also called a hypnotic. It affects chemicals and cause sleep problems (insomnia). Ambien is used to treat insomnia.

Packages:
M2B is offering small, regular and bulk quantity customers can view our list


Shipping Area:
We ship from USA,UK and Philippines.

Note:
Product delivered can be different from the image listed. We try our level best in any case if you are not satisfied please contact us before throwing a negative feedback

Email ID : [redacted]@safe-mail.net

FORUMS MEMBERS

Mark Forums Read Search Forums Watched Forums Watched Threads New Posts



Member
Vendor

Joined: Mar 18, 2015
Messages: 218
Likes Received: 31

I'm interested in Medical Doctors license number, NPI numbers and most importantly, DEA numbers. If anyone can get this info, you will have a place to sell them right here.

Anyone know of a source of this sort of information?

Maybe a hospital/pharmacy's computer can be penetrated...

contact me via jabber [email]@im-koderoot.net/email

JABBER+city only. NO IQQ > PM me for username, or for any business also for any questions. I will do my best to answer. Knowledge is power. Sharing is caring. growdy, shady mother fuckers around here killing the collaboration... and the community along life...

May 26, 2015

Report Like Reply #1

Threat Actors and Motives

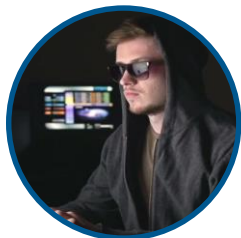


Activist Arthur

Motive: Social, political, or religious justice

Skill: Varied

Tactic: Website defacement, social media hijacking, visible damage



Script Kiddie Sal

Motive: Curiosity, thrill, or ego

Skills: Basic security / computer skills

Tactic: Pursues targets of opportunity, not targets of choice



Big Money Mabel

Motive: Financial gain

Skills: Moderate – Advanced, organized

Tactic: Extortion, fraud via opportunistic, broad phishing, ransomware, malware



Nation State Cyber Crime

Motive: Military intelligence, nationalism

Skills: Advanced, highly funded

Tactic: Targeted advanced threats



Negligent Ned

Motive: Get it done!

Skills: Varied

Tactic: Improper data handling



Malicious Molly

Motive: Personal gain, career advancement

Skills: Limited

Tactic: Data exfiltration

INSIDERS

Threat Actors and Motives



Activist Arthur

Motive: Social, political, or religious justice
Skill: Varied

Tactic: Website defacement, social media hijacking, visible damage



Script Kiddie Sal

Motive: Curiosity, thrill, or ego
Skills: Basic security / computer skills
Tactic: Pursues targets of opportunity, not targets of choice



Big Money Mabel

Motive: Financial gain
Skills: Moderate – Advanced, organized
Tactic: Extortion, fraud via opportunistic, broad phishing, ransomware, malware



Nation State Cyber Crime

Motive: Military intelligence, nationalism
Skills: Advanced, highly funded
Tactic: Targeted advanced threats



Negligent Ned

Motive: Get it done!
Skills: Varied
Tactic: Improper data handling



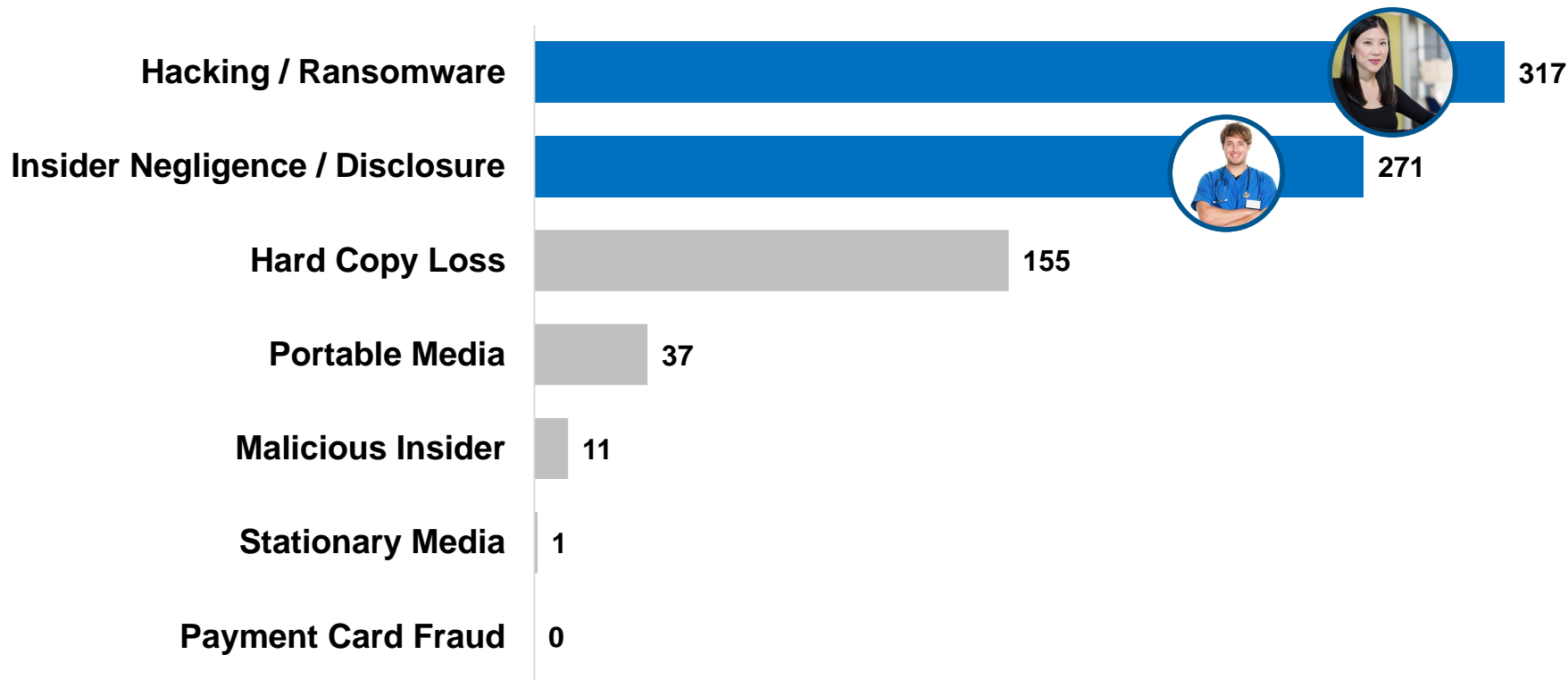
Malicious Molly

Motive: Person gain, career advancement
Skills: Limited
Tactic: Data exfiltration

INSIDERS

Healthcare and Non Profit Data Breach Events

Jan 2016 - Oct 2017



Privacy Rights Clearinghouse <https://www.privacyrights.org/data-breaches>



Big Money Mabel

Motive: Financial gain

Skills: Moderate – Advanced, organized

Tactic: Extortion, fraud via opportunistic, broad phishing, ransomware, malware

Big Money Mabel – Ransomware Phish



From: HR Department <hr@hr-communication.com>

Subject: Election Policies

Hi team,

In preparation for election day, we have outlined our company policies in the portal.

Please be advised of our non-solicitation policies that require employees to refrain from activities including passing out political literature during work hours, excluding breaks. We have established a neutral dress code that prohibits the wearing of buttons, badges, or other political dress. Those who are not in compliance with our policies will be disciplined if the conduct creates a disruption in the workplace.

To record your acknowledgment, visit the [portal](#). All employees are required to sign this document by COB.

We appreciate your cooperation. Your efforts help us foster our inclusive culture of diversity and mutual respect.

17.28% Industry Susceptibility



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

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

GMT from Monday to Friday

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

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt



Negligent Ned

Motive: Get it done!

Skills: Varied

Tactic: Improper data handling

Top Causes for Negligent Data Disclosure



1. IT Systems Administrator improperly configures systems
2. Credential Sharing to Medical Records Systems
3. Misdirected email of health information

Protect Your Credentials




- *Health Informatics Research* survey of medical staff
- Willingness to share credentials to PHI
- Results indicated:
 - 74% of health professionals admit to using the credential of another medical staff member; 4.75 times on average.
 - 100% of medical residents obtained a credential from another medical staff member, while only 58% of nurses claimed to use a borrowed credential
 - Job duties exceed access rights - #1 reason for borrowing credentials


Protect Your Credentials



NATIONAL MARROW DONOR PROGRAM®

BE  THE MATCH®

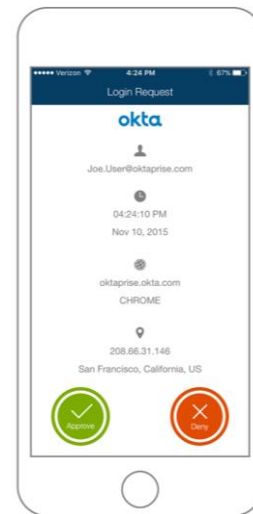
Welcome to the
National Marrow Donor
Program



SecurID Username

SecurID PIN + Passcode

Sign In



Reminder: Network Partners are responsible for protecting credentials and notifying Be The Match of personnel changes and terminations.

Thank You for Attending



Heather Helm

Product Owner, Donor Services
NMDP / Be The Match
Email: hhelm@nmdp.org



Rob Hanson

Information Security and Data Privacy Director
NMDP / Be The Match
Email: rhanson@nmdp.org

References

- [Healthcare Informatics Research: Prevalence of Sharing Access Credentials in Electronic Medical Records](#)
- [Cybercrime and Other Threats Faced by the Healthcare Industry](#)
- [Health Warning Cyberattacks are targeting the health care industry](#)

Evaluation Reminder

Please complete the Council Meeting 2017 evaluation in order to receive continuing education credits and to provide suggestions for future topics.

We appreciate your feedback!