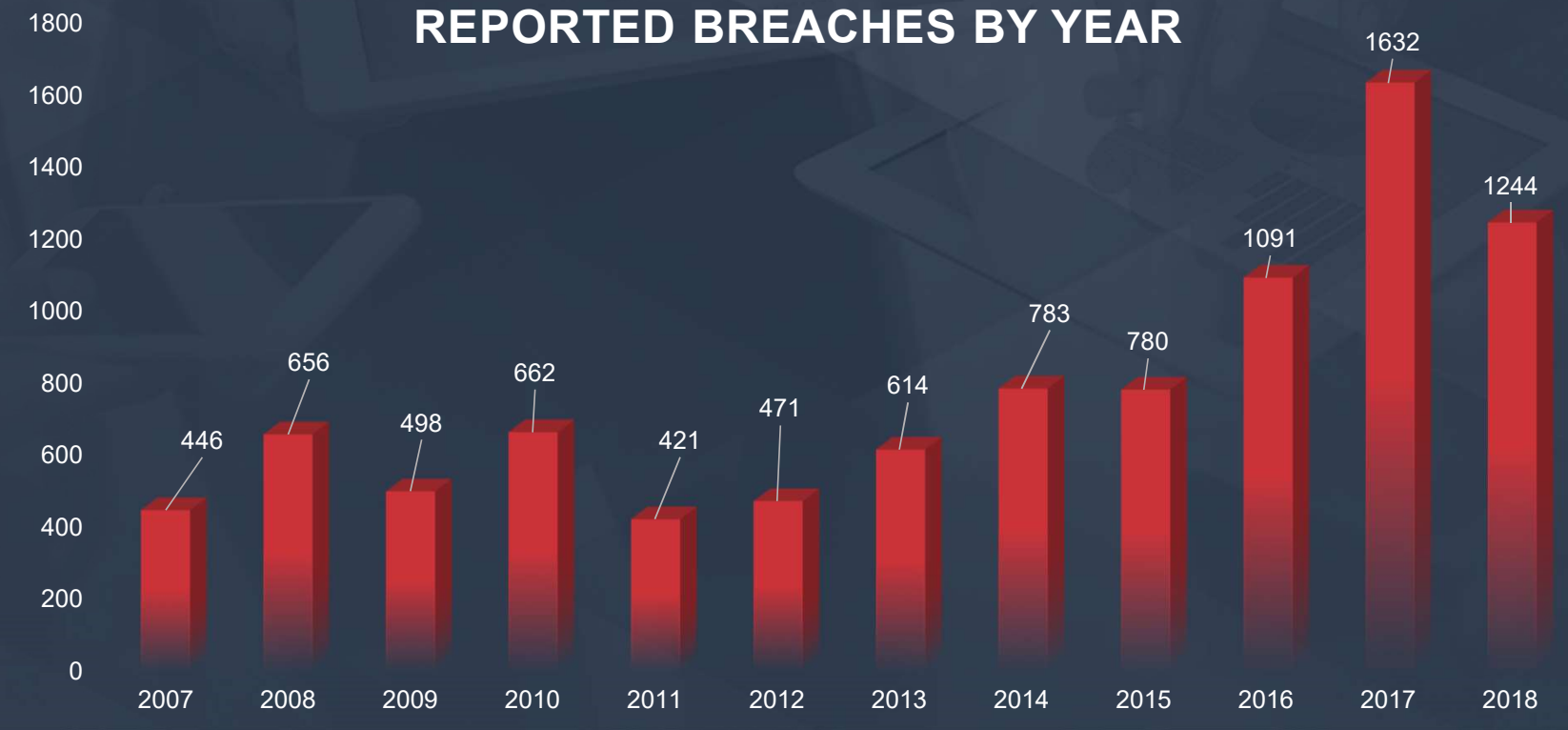
Dark Web: More Connected More At Risk

Addressing Cybersecurity Concerns for Your Organization

May 7, 2019

Latest Statistics Show Less Breaches



However, the Impact is More

2017

1,632 breaches reported

197,612,748 exposed records

2018

1,244 breaches reported

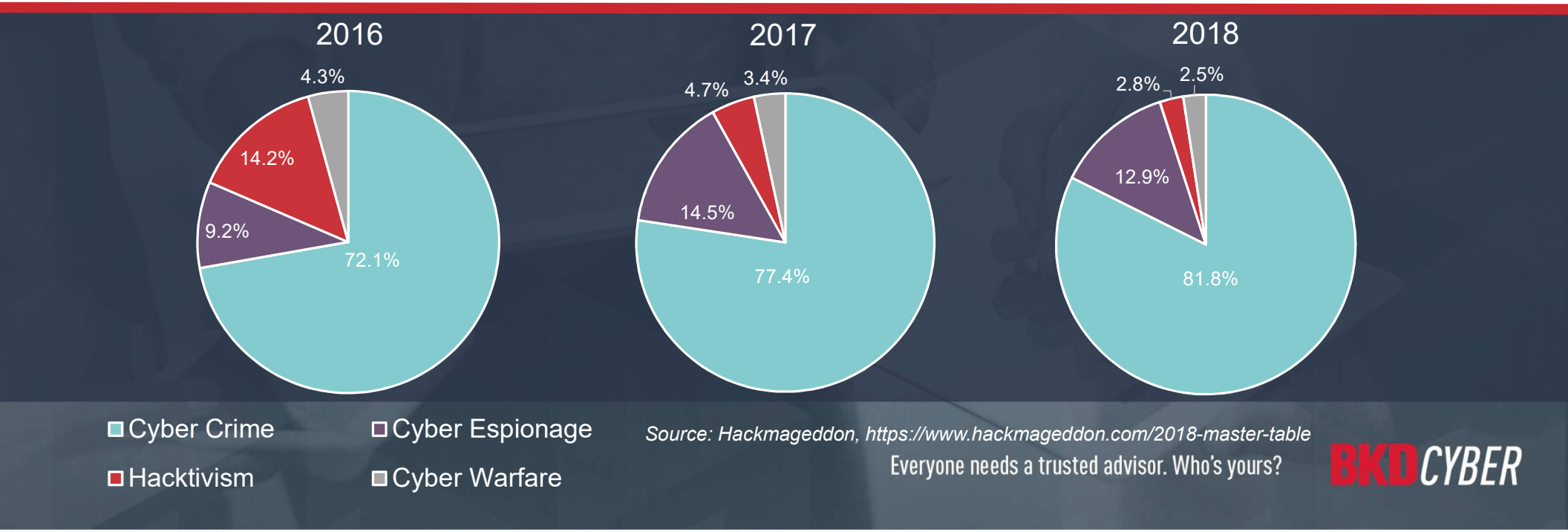
446,515,331 exposed record

*2018 had over **2.25** times more records exposed in **76%** of the number of breaches*

Source: https://www.idtheftcenter.org/2018-data-breaches

Cyber Crime is Still the #1 & Growing

Motivations Behind Attacks



Source: Hackmageddon, https://www.hackmageddon.com/2018-master-table

Everyone needs a trusted advisor. Who's yours?

BKD CYBER

Breaches Are Costing More & More

Average total cost of a data breach
$3.86 million

Up from $3.62 million

Average cost per lost or stolen record
$148

2017 was $141

Likelihood of a recurring breach within two years
27.9%

27.7% last year

Mean time to identify a breach
197 days

Mean time to contain
69 day

Average cost savings with an IR team
$14/record

Companies that contained a breach in less than 30 days saved more than $1 million vs. those that took more than 30 days to resolve

Source: Ponemon Institute 2018 Cost of Data Breach Study

The Dark Web

What it is, & what it isn't

Everyone needs a trusted advisor. Who's yours?

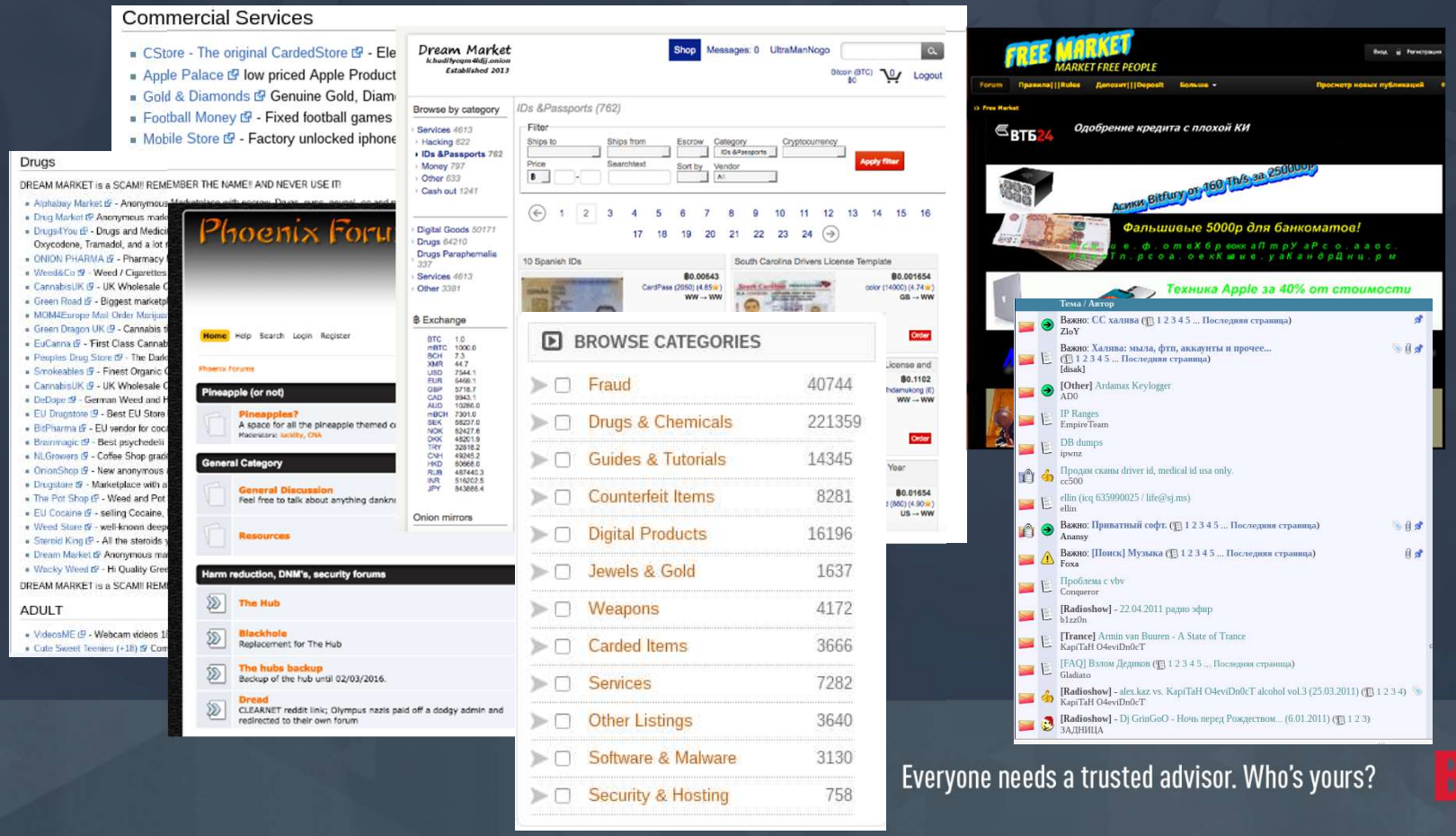
BKD CYBER

What is the “Dark Web”?

- Less than 10% of the internet is accessible through typical search engines
- The **Deep Web** is a part of the web that contains the most sensitive information
- The **Dark Web** is the part of the deep web that is intentionally hidden
- Requiring an ***anonymizer*** to access (ex. Tor)
  - Uses .onion link; links often shift
  - **Tor –** The Onion Router
  - **<u>The Black Market of the Internet!</u>**

Source: CISO Platform
http://www.cisoplatform.com/profiles/ blogs/surface-web-deep-web-and-dark-web-are-they-different

What Can I Find on the Dark Web?



Types of Sites on the Dark Web

Forums

Discussion forums that cover information that could be useful to a hacker

- Common vulnerabilities
- Information about organizations

Search Engines

Just like regular search sites, but for the dark web

Marketplace

Anything is for sale

- Drugs
- Stolen credit cards
- Personal identities
  - Passports
  - Driver's licenses
  - Health insurance cards
- Other compromised information
- Dates

Paste Sites

Large data dumps that are never removed

Social Media/Chat Rooms

A place for hackers to share information more privately

Some Items for Sale

Directv Account with NFL SUNDAY TICKET MAX

Vendor	kingshot (3200) (4.72⭐) (ⓐ 388/3/16) (♥ 1307/25/25)
Price	฿0.00489 ($18.72)
Ships to	Worldwide
Ships from	Worldwide
Escrow	No

Product description

"Directv goes everywhere you go. Stream live TV, access shows and movies On Demand, 100s of channels to choose from."
Account with NFL SUNDAY TICKET MAX subscription guaranteed

Buy this account now for a fraction of the price.
-High Quality
-Fast delivery

Spotify - premium account - lifetime

Vendor	K2000 (780) (4.90⭐) (ⓐ 119/0/2)
Price	฿0.001358 ($5.2)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	Yes

Product description

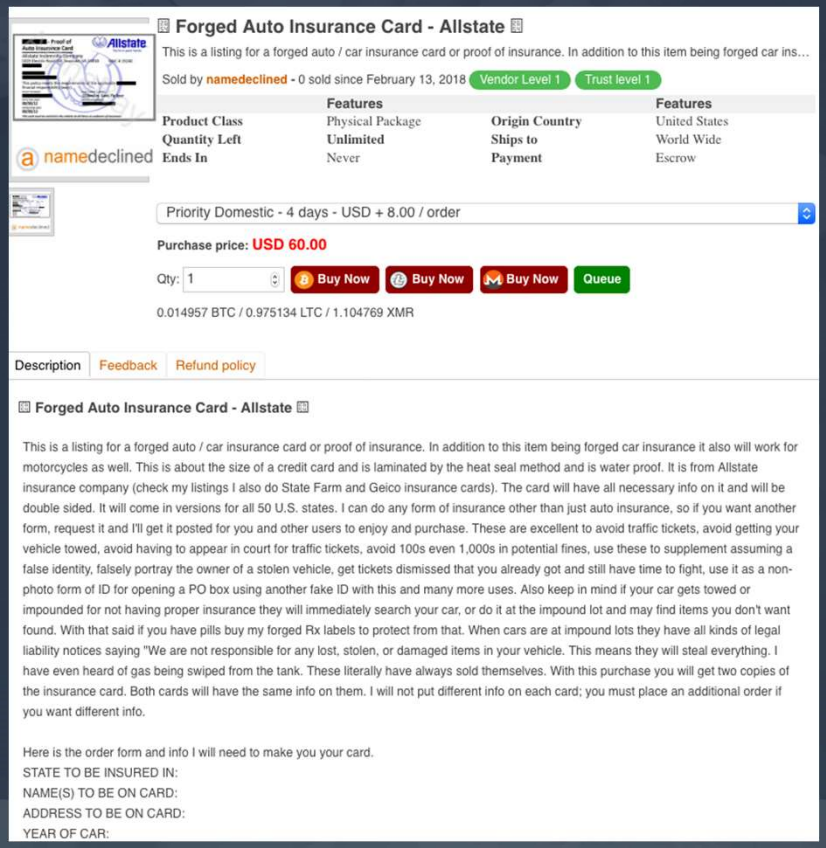
Spotify - premium account - lifetime

Your purchase includes:
- Full Access to premium account.
- Lifetime warranty

Username and Password are sent via PM.

All images are actual screenshots from the dark web

Fake Insurance Card

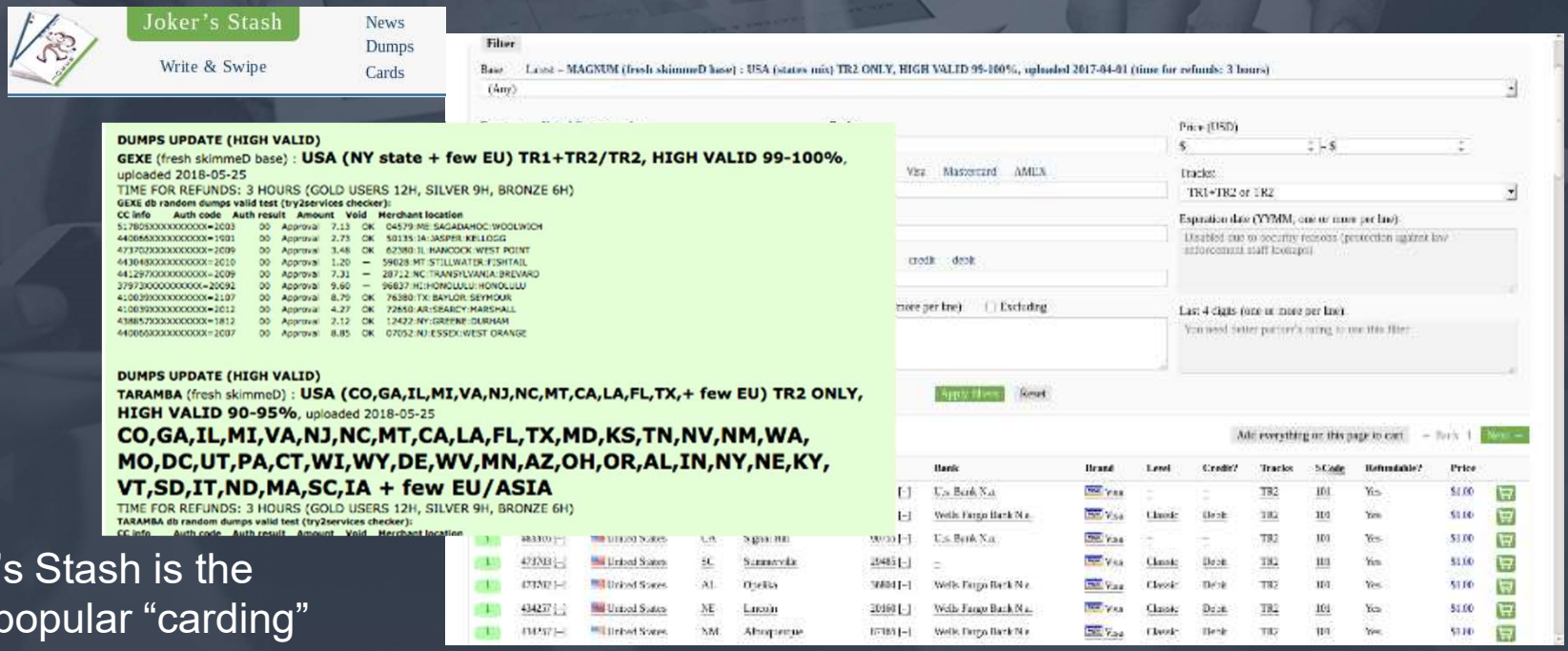


All images are actual screenshots from the dark web

How Much Could I Get for Your Credit Card On the Dark Web?

About $1

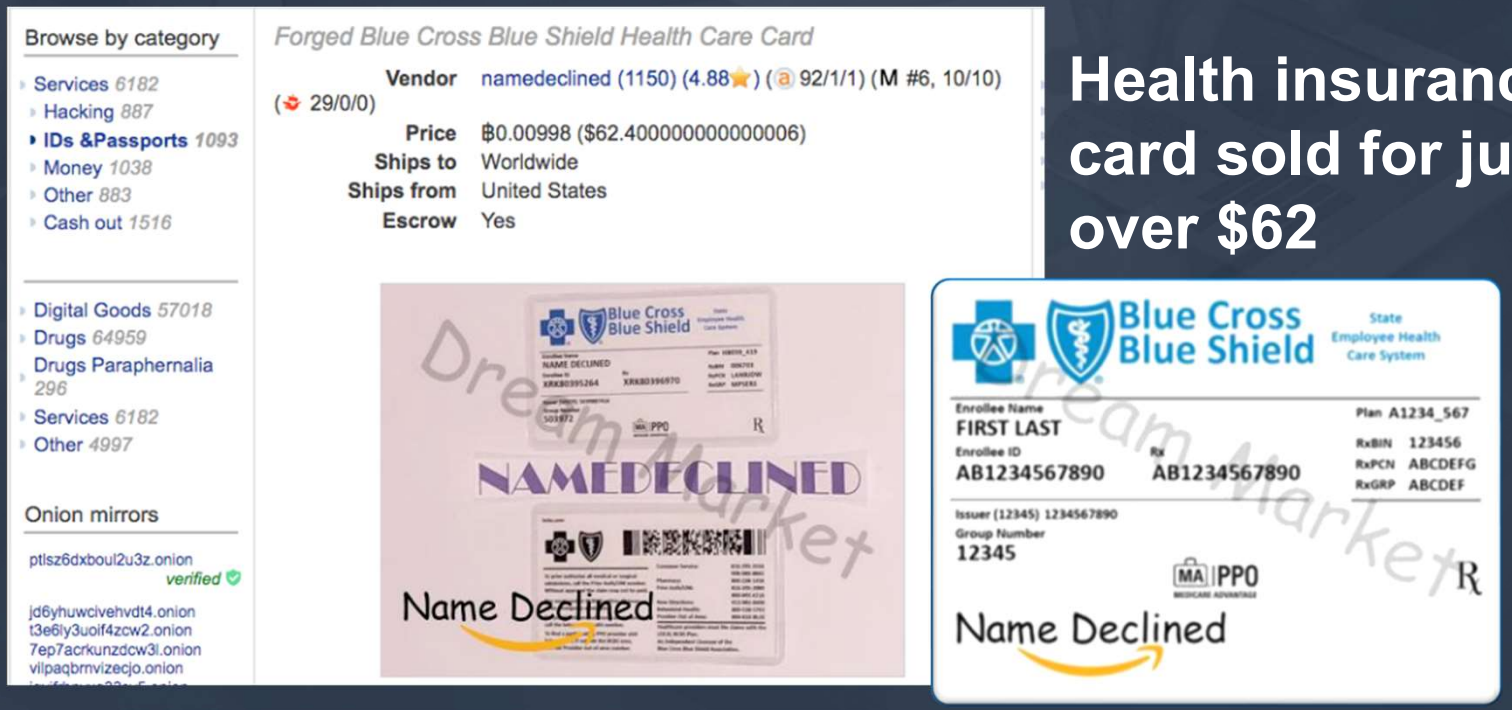
Carding Forum



Joker's Stash is the most popular "carding" forum on the dark web. Credit cards, just $1 each!

All images are actual screenshots from the dark web

Carding Forum



Health insurance card sold for just over $62

Health Insurance Card for Sale

Product description

This listing is for a forged Blue Cross Blue Shield health insurance card / proof of insurance card. These cards are printed double sided and are plastic heat laminated cards. They are waterproof and you will get two cards with the order; both cards will be identical and the second is just a spare or back up in case the first is lost, stolen, damaged, has a defect or is ceased. The back of the card will scan with all the proper info so if real info is used it will show up in the system, or even smart phone applications may be used to scan and read the back of it.These are use to provide proof that you have health insurance in the United States (BCBS may exist outside the US and can be forged to be used outside the US) This item works very well as a back up form of ID to pair with a fake drivers license or fake passport or even one of my forged drivers license, social security cards, auto insurance cards, or school IDs. When using a fake ID or assuming a fake identity it is best to not have a wallet that has simply cash and a fake drivers license only. Having a forged health care card and other forged IDs of mine along with maybe a prepaid debit card from your local store sell your cover identity. If your fake ID is questioned this can be pulled out to back it up and eliminate any question, it may save you. In addition it may be used as a secondary form of ID to open up a PO box under a false identity and fake info. Keep in mind that the post office does not cross check the info you provide them when opening a PO box they merely take down the info that they view on your IDs and log it in the computer. They do not have the power to access BCBS databases to verify nor do they verify any of the info. If say by chance you are able to steal info about a real BCBS insurance policy you may use that info and get a fake from me and use that policy and assume that persons policy, possibly even get a few visits covered before they catch on.

Hackers for Hire

Government is chasing me - Need Help

@uniter 6 мес. назад

I've been extensively chased by the government for 7 months now...
I'm writing this, not interested in a debate or needing to vindicate what I'm claiming. And before this gets to a discussion about my sanity. I am not schizophrenic or any type of mentally ill. Very sane in fact... All of this is happening as described. I am telling nothing but the truth and I am ONLY writing this because I have to reach out to a community of people that can some-what understand .
I am not writing this for attention, or for any sort of egotistical getting my rocks off sort of thing. I'm hoping some open minded people will respond to this because I really need help in the ways that I'm asking.

I desperately need help. I've been running from them for 6-7 months now, chased across north america from coast to coast twice now without money, without food, no resources. It's been hard...
I cannot name the names of the agencies doing this or WHY this is happening, but there are multiple groups working together in different capacities spearheaded by one agency specifically in charge of this all. Please don't ask, that's all I can say.

When this all started, it was just them watching me mostly - and fucking with me / all the people that I was involved with. Trying to intimidate me and my friends. They were Deleting tax records, bank accounts, social's, etc. Stalking and breaking into our houses, etc.
All my friends / people I knew were hacked into from the nsa and we were all being monitored by agencies outside of the nsa who were working with the nsa to use their technology to track us and monitor everyone. The people closest to me were on high priority watch lists and anyone that was involved with what I was doing / knew.
Were being attacked the same way that I was. A few of us had / have our lives at stake right now.

Rent-A-Hacker

Products | FAQs | Register | Login

Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:
Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.
Im a proffessional computer expert who could earn 50-100 euro an hour with a legal job.
So stop reading if you dont have a serious problem worth spending some cash at.
Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.
You can pay me anonymously using Bitcoin.

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successfull, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

Social Engineering skills:
- Very good written and spoken (phone calls) english and german
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt belive really often.
- Alot of experience with security practices inside big corporations.

What ill do:
Ill do anything for money, im not a p[illegible] :-) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone
Ruining your opponents bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.

How Are You Targeted?

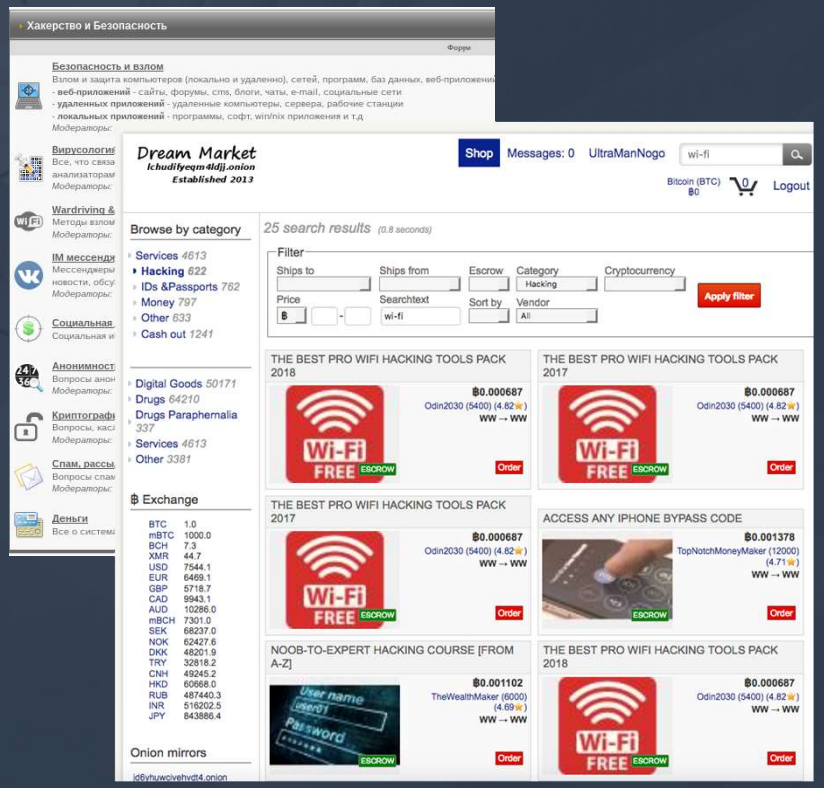
Things to look out for…

Everyone needs a trusted advisor. Who's yours?

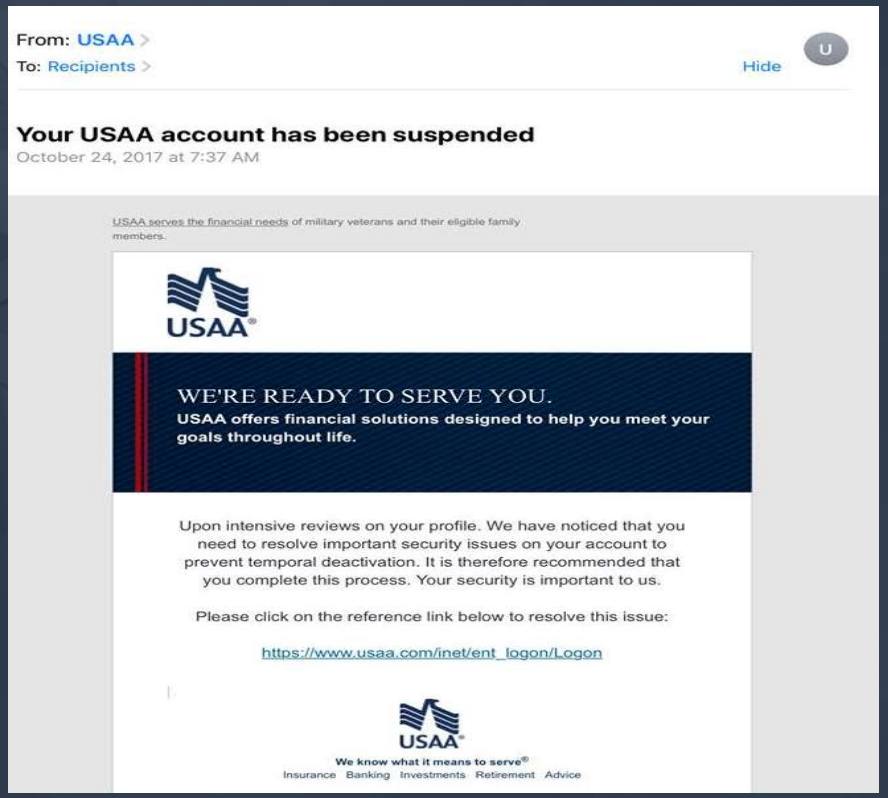
BKD CYBER

Attackers Try Easiest Way to Penetrate

- Phishing/spear phishing
- Social engineering
  - Job opportunities
  - Accounts on LinkedIn, Facebook
- Malware campaigns
- SQL injections on websites
- Public Wi-Fi



Phishing Schemes are Most Popular



From: USAA >
To: Recipients >
Hide

Your USAA account has been suspended
October 24, 2017 at 7:37 AM

USAA serves the financial needs of military veterans and their eligible family members.

USAA

WE'RE READY TO SERVE YOU.
USAA offers financial solutions designed to help you meet your goals throughout life.

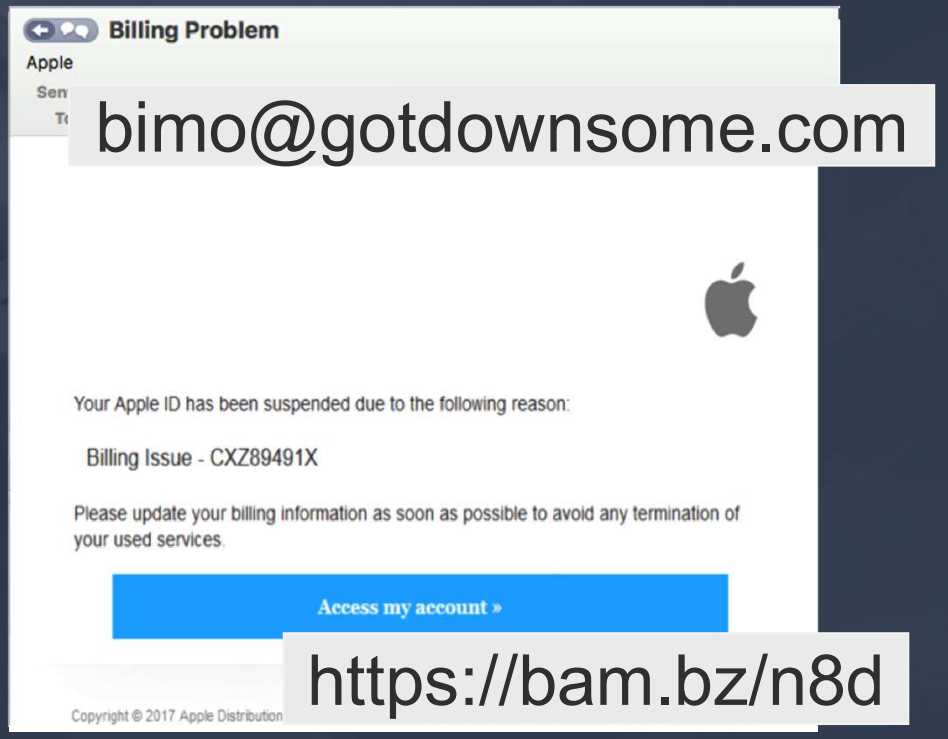
Upon intensive reviews on your profile. We have noticed that you need to resolve important security issues on your account to prevent temporal deactivation. It is therefore recommended that you complete this process. Your security is important to us.

Please click on the reference link below to resolve this issue:

https://www.usaa.com/inet/ent_logon/Logon

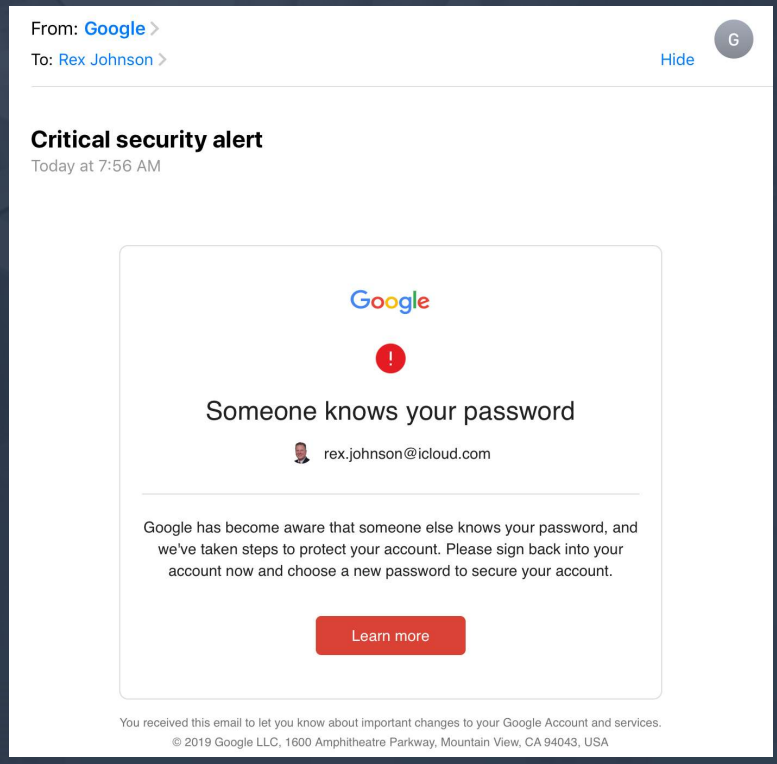
USAA
We know what it means to serve®
Insurance Banking Investments Retirement Advice

Always Check…



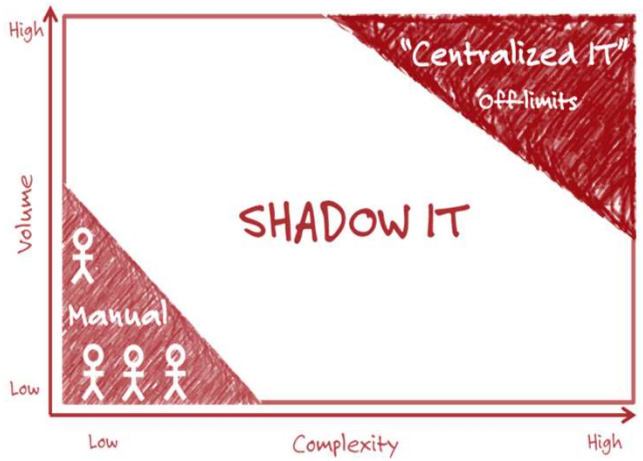
Some Emails Are Legitimate, but…

- Never select the link in the email
- Call or go to a site that you know is official



Shadow IT

- Shadow IT refers to IT devices, software & services outside the ownership or control of IT organizations
- Departments will often do this to
  - Circumvent bottlenecks
  - Avoid slow processes
  - Rely on familiar software
  - Compatible with mobile devices
  - Work with legacy applications that are no longer supported
- It is easy to attain software as a service (SaaS) solutions



Source: Gartner IT Glossary, https://www.gartner.com/it-glossary/shadow

Risks of Shadow IT

- Rutter Networking identified
  - Increased risk of data loss
  - Increased risk of data breach
  - Inefficiencies
  - Cybersecurity risks

- Since acquired outside of IT procurement channels, security is often overlooked
- Gartner predicts that by 2020, a third of all successful attacks will be against their shadow IT resources

Source: https://www.rutter-net.com/blog/4-security-risks-of-shadow-it

What Would a Hacker Take?

Knowing how a hacker would compromise your environment

Everyone needs a trusted advisor. Who's yours?

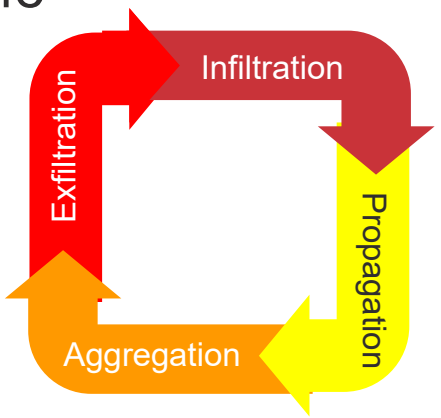
BKD CYBER

Red Team Digital Attack Simulation

- An attack simulation that mimics the real activities a hacker would take in your environment.
- Still provides the network penetration testing results
- Collects data and information a hacker would want
- Ability to place notional malware and threats
- Also known as Purple Team or Digital Attack Simulations

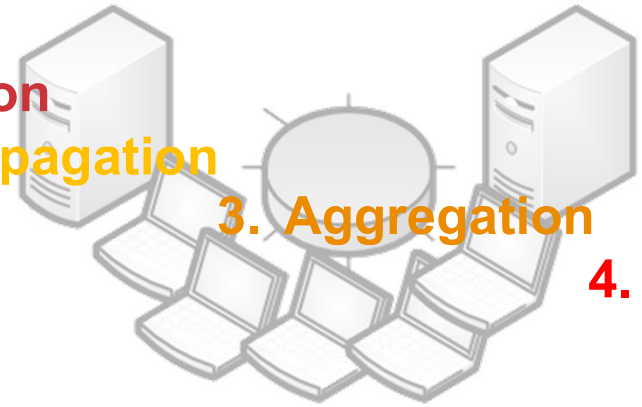
Breach Life Cycle

- Attacks are generally carried out in four stages
- These four stages are often referred to as the “breach life cycle”
- The further the progression, the greater the risks
  - Infiltration: breaking in & establishing foothold
  - Propagation: in the network & moving around
  - Aggregation: collecting data & critical information
  - Exfiltration: taking the information outside of the organization



Breach Life Cycle in Action

1. Infiltration
2. Propagation
3. Aggregation
4. Exfiltration



How the Red Team Works

Leadership engages red team

Red team hackers break in (infiltrate)

Red team propagates & aggregates

Once detected, red team shows exfiltration data

Provides feedback to security team

Publishes the report

Red Team Benefits

- Simulated attack scenarios from real-world threats
- Demonstrates true offensive techniques to organizations
- Identify return on investment for cybersecurity solutions
- True ‘quantitative’ risk analysis
- Focuses on what’s valuable, data & assets
- Designed to improve a security team
- Still get the penetration test report plus more

Mitigation Steps

A few things you can do to reduce risk…

Know Your Inventory

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- Classification of inventory

Educate Your Team

- Technology is no substitute for employee education
- Include the board, executives & vendors
- Knowledge is power
- Do not discourage false-positive reporting
- Document & distribute security policies
- Develop & rehearse a robust incident response program

Patch Your Systems

- Applications
- Databases
- Operating systems – servers, workstations, etc.
- Anti-virus/anti-malware – engines & signatures
- Third-party applications

Limit Access

- Control use of administrative privileges
- Limit access based on need-to-know (least privilege)
- Limit & control remote access
- Do not share credentials
- Consider multifactor authentication
- Limit the use of portable media
- Don’t forget physical security
- Encryption is key, especially when data leaves your organization

Human Fact is Still the Weakest Link

- Remember physical security & limiting access when the following arrive
  - UPS
  - Coming in from corporate IT
  - Service people or technicians
  - Exterminator
  - Flower delivery

Plan, Prevent & Prepare

- Lock your laptop whenever you are away from your workstation
- Filter out suspicious email addressed to employees
- Be careful how you share company information
- Develop cyber incident response program (CIRT)
- Consider cyber insurance

Backup

- Implement a regularly scheduled backup program that meets your business & records retention requirements
- Put some distance between your primary & secondary sites
- For critical applications, perform a full restoration or fail-over test at least annually
- Backup & restore not only data, but also the applications
- Understand the differences between cloud storage & cloud backup

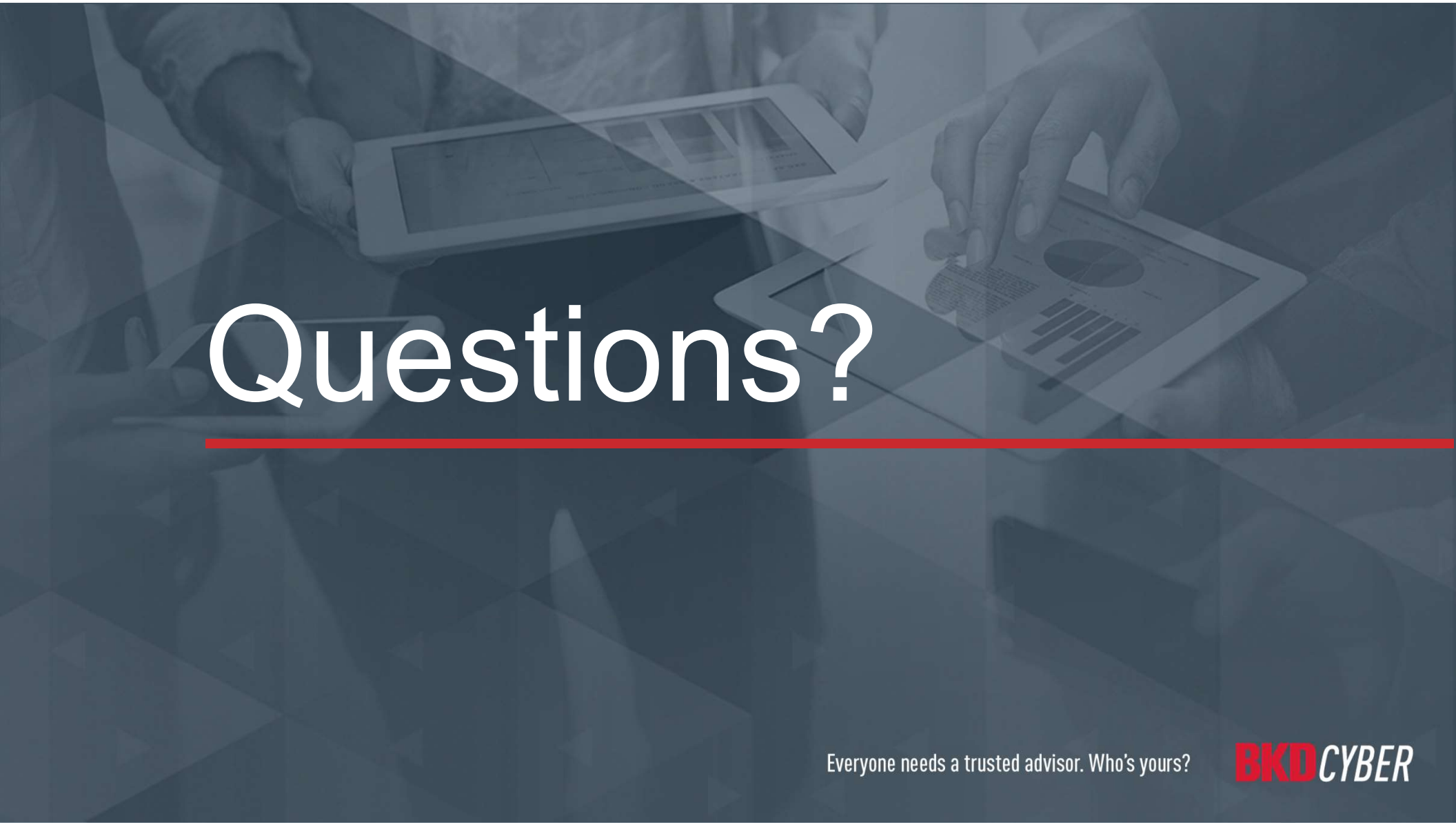
Personal Recommendations

- Always ask why someone needs your information
- Avoid clicking links within unsolicited emails or text messages; go to the legitimate site & type in URL
  - https://www.bankofamerica.com – correct
  - http://www.bankofmerica.com – incorrect
- ***Be aware of cyber fatigue in your organization***
- Use strong passwords & change them often
- Avoid geolocation tagging in photos or tweets
- **Don't talk publicly about your company**: happy hours are perfect targets

The Next Generation

- CyberPatriot is the National Youth Cyber Education Program
- Created by the US Air Force and sponsored by Northrop Grumman
- Inspires K-12 students towards careers in cybersecurity or other science, technology, engineering, and mathematics (STEM)
- Preparing youth with skills critical to our future

https://www.uscyberpatriot.org/
http://www.northropgrumman.com/CorporateResponsibility/Pages/CyberPatriot.aspx


Questions?
Everyone needs a trusted advisor. Who's yours?
BKD CYBER

Thank you!

bkd.com | @BKDLLP @RexSecurity @BKDCyber

Everyone needs a trusted advisor. Who's yours?

BKD CYBER