



# CYBER INSIGHTS

*IS YOUR CYBER SECURITY AT RISK?*

VOLUME 2 • ISSUE 2 • JUNE 2018

## **FRAUD OR FACT**

## **THE BASICS**

### DEFINING CYBERSECURITY (by HOMELAND SECURITY)

**Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.**

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.



## FRAUD OR FACT

## THE BASICS

# SOCIAL ENGINEERING

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. People with an online accounts, social media, or any online presence should watch for phishing attacks and other forms of social engineering.

## THE “DARK WEB”

The “[dark web](#)” is a part of the world wide web that requires special software to access. Once inside, web sites and other services can be accessed through a browser in much the same way as the normal web.

However, some sites are effectively “hidden”, in that they have not been indexed by a search engine and can only be accessed if you know the address of the site. Special markets also operate within the dark web called, “darknet markets”, which mainly sell illegal products like drugs and firearms, paid for in the cryptocurrency [Bitcoin](#).

There is even a crowdfunded “[Assassination Market](#)”, where users can pay towards having someone assassinated.




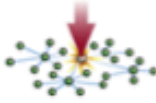






Because of the the dark web’s almost total anonymity, it has been the place of choice for groups wanting to stay hidden online from governments and law enforcement agencies. On the one hand there have been whistleblowers using the dark web to communicate with journalists, but more frequently it has been used by [paedophile groups](#), [terrorists](#) and [criminals](#) to keep their dealings secret.



# FRAUD OR FACT

# THE BASICS

## Types of Attacks?







	DDoS		False Tax Return Filings
	Doxing		Network Destruction Attacks
	Theft of IP		Ransomware and Extortion
	Theft of PII, PHI		Business E-mail Compromise
	Point of Sale Breaches		Website Defacements



# FRAUD OR FACT

# THE BASICS

## Who may be doing the hacking?

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hackers might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



## FRAUD OR FACT

### Crimes are not only for money but also for your data

## Terminology - NPPI & PII Defined

#### Non-public Personal Information (“NPPI”):

Personally identifiable data such as information provided by a customer on a form or application, information about a customer’s transactions, or any other information about a customer which is otherwise unavailable to the general public.

NPPI includes first name or first initial and last name coupled with any of the following:

- Social Security Number

- Driver’s license number

- State-issued ID number

- Credit or debit card number

- Other financial account numbers

NYS DFS CyberSecurity Amended Regulations: Have narrowed their broad definition of Nonpublic Information to “Business Related” information (§500.01 (g)) (earlier version covered “any information, not nonpublic or business-related information).

#### Personally identifiable information (PII):

Any data that could potentially identify a specific individual.

Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered **PII**



## Cyber Insurance

## Get a better understanding

- Cyber Insurance still in “wild west” territory, but improving.
- Don’t purchase without reviewing current policy; consulting specialist.
- Policies may become outdated quickly in light of new threats, so review regularly.
- Be aware of what’s covered. Notice requirement costs? More?



## Cyber Insurance

## Get a better understanding

**Medidata Solutions Inc. v. Federal Insurance Co.** - *finance department deceived into transferring \$4.8 million to a Chinese bank account*

*There was no manipulation of computers*

**Vs**

*“voluntarily” transferring funds by authorized parties*

## FRAUD OR FACT

This is why human error is so important – if someone in your office ‘clicks’ a bad link, then your agency may not have coverage for that error or cyber event that leads to hacked emails, diverted wire transfers or breach of private data.



## Cyber Insurance

## Get a better understanding

- Ensure E&O covers defense for suits related to alleged negligent acts leading to breach or other cyber crime.
- Crime coverage (also called “fidelity” insurance) and cyber policies can cover first-party losses for social engineering.
- At this time, coverage for direct third party losses caused by “social engineering” scams (e.g., a client’s loss via wire fraud) may not exist.





## Cyber Insurance

## Get a better understanding

Cyber liability provides coverage for the theft of your customers' non-public information NOT the theft of your customers' escrow funds.

Cyber Liability provides coverage in the event you suffer a security breach, your customers' non-public information is compromised and they sue you for damages and expenses. These costs are covered under the following Cyber Liability policy insuring agreements:

- ❖ Security and Privacy Liability
- ❖ Privacy Regulatory Defense & Penalties
- ❖ Data Recovery - *Ransomware*
- ❖ Customer Notification and Credit Monitoring Costs
- ❖ Data Extortion/Ransomware
- ❖ Multimedia Liability



## FRAUD OR FACT

## FUTURE IMPROVEMENTS

# Help is coming in 2018 with Wi-Fi Protected Access 3

- WPA3 protocol strengthens user privacy in open networks through individualized data encryption.
- WPA3 protocol will also protect against brute-force dictionary attacks, preventing hackers from making multiple login attempts by using commonly used passwords.
- WPA3 protocol also offers simplified security for devices that often have no display for configuring security settings, i.e. IoT devices.
- Finally, there will be a 192-bit security suite for protecting Wi-Fi users' networks with higher security requirements, such as government, defense and industrial organizations.





# CYBER INSIGHTS

*IS YOUR CYBER SECURITY AT RISK?*

VOLUME 2 • ISSUE 2 • JUNE 2018

## **FRAUD OR FACT**

PROTECT YOURSELF  
PROTECT YOUR BUSINESS  
PROTECT YOUR CUSTOMER  
PROTECT YOUR FUTURE

STAY INFORMED

