In the new CYBERCRIME ERA

PROTECTING YOUR RETIREMENT SAVINGS
Today, in every part of business and our daily lives, the convenience and access of modern technology is also exposing us to an unprecedented level of personal risk. It is more than the threat of a stolen cell phone... it could be a major bank you trust suffering a critical hack that destroys all records of your accounts.

Our credit, our identities, the ability to buy and sell in financial accounts, our children’s college funds, our private email correspondence: all of it is now within the reach of the new breed of sophisticated cyber criminals.

No wonder that cybercrime has surpassed illegal drug trafficking as the number one way for criminals to earn money. In fact, you are more likely to get your email account hacked into than to suffer a home break-in.

With this threat growing every day, it pays to get informed and prepared now. Don’t wait until your bank’s systems are compromised to get serious about protecting your family from cybercrime.

Cybercrime is defined as a criminal activity using a computer and a network that involves:

- Hacking
- Copyright infringement
- Cyber stalking
- Bullying
- Theft of data
- Terrorism
- Government & corporate espionage
- Extortion

CALL 800.462.0071 FOR YOUR FREE CONSULTATION
LEARN THE FACTS

According to Juniper Research, the global cost of cybercrime will reach $2 trillion by 2019, a threefold increase, from the 2015 estimate of $500 billion. In fact, more than 29 million records were exposed in 858 publicized breaches across all sectors of the economy. (Source: Theft Resource Center).

A significant portion of cybercrime goes undetected and this is particularly true for industrial espionage where sensitive records are involved. The average cost of a typical security breach was $4 million and more than $7 million in the United States. (Source: Poneman Institute). The financial hit resulting from the loss of trade secrets ranges from 1 percent to 3 percent of an entire nation’s gross domestic product. In 2016, cyber security incidents rose 38 percent than in the previous year. (Source: IDG).

Today, U.S. state and local law enforcement, telecommunications companies, Internet application developers and private data aggregators are gathering vast amounts of personal data about you and those you love including what you buy and sell, how you spend and how invest.

HOW SAFE IS YOUR PERSONAL INFORMATION?

About 1 in every 16 U.S. adults were victims of ID theft last year (6.15%) – and the incidence rate jumped some 16% year over year. This despite 2016 being the first full year that retailers were forced to accept more secure EMV chip cards or face liability consequences. (Source: credit.com)
In 2015, nearly 300 million records were leaked and more than $1 billion dollars was stolen because of cyber attacks. The following chart shows other significant security breaches and the amount of personal records stolen:

**SELECTED DATA BREACHES**  
(as of February 2016; in millions of dollars)

- **U.S. Voter Database**: 191 (December 2015) 152
- **Ebay**: 145 (March 2014) 130
- **T.J. Maxx**: 94 (March 2007) 92
- **Anthem**: 80 (February 2015) 77
- **U.S. Military**: 76 (January 2009) 76

Source: Statista.com
WHY IS CYBERCRIME SO DIFFICULT TO FIGHT?

The image of the lone hacker working out of a bedroom could not be farther from the truth. Today, cyber criminals are sophisticated professionals who work in trans-national organizations difficult to trace and virtually impossible to prosecute. More than 70% of cyber crime crosses national borders. Because the laws between countries vary regarding digital crime, it can be difficult if not impossible to bring cyber criminals to justice. In fact, 25% of all cyber crimes go unsolved. (Source: Forbes)

WHAT YOU CAN DO TO PROTECT YOURSELF AGAINST CYBERCRIME

Keeping your online identity and privacy should be a top priority. The key: Be proactive and vigilant. Beware of web sites that offer a reward or prize in exchange for your personal details. Don’t reply to spammers for any reason. Never reveal any personal information online inadvertently. Try to stay on top of computer and network security issues.

No matter what you do, you are still at risk of security lapses from family, friends and colleagues and you may become a victim of cybercrime despite your best efforts.

So far in 2017, cyber attacks are rising at an alarming rate. Cyberwarfare is at an all-time high, and cybersecurity is just unable—unequipped—to keep up. We’re seeing a convergence of three major vectors—devices, data, and a shortage of talent—coming to a head. That’s causing an explosion of cybercrime. (Source: Forbes)

The financial industry suffers constantly from web app attacks, denial of service attacks, card skimmers, employee privilege misuse, and crime ware. Even the most powerful politicians in Washington are unable to keep their emails private. The Panama Papers—a set of 11.5 million confidential documents that show how wealthy individuals and some public officials hide assets from public scrutiny—just gave us our largest data leak in history.
GOLD: THE ASSET THAT CAN’T BE THE VICTIM OF A CYBERCRIME

One day you might go to your ATM and find the system will be down because of a cyber attack. Or you may experience a computer shutdown due to malware or a Trojan horse hack. What happens to your business and your lifeline to your loved ones when your debit card or cell phone is hijacked? Cyber criminals can hack your data, steal your identity and put your hard-earned wealth at risk.

Smart investors know there is a way to shield their financial affairs from cyber criminals. They turn to an asset that no government, corporation or hacker controls: gold. The global market for gold is large and liquid. Reputable gold dealers operate in every major country.

In the event of a large scale hacking attack on the financial industry, what could provide more comfort than physical gold and silver in the home safe or in your IRA. Gold coins are interchangeable and can be easily stored or hidden in case of a cyber attack.

The case for owning gold has grown stronger in recent months. As recessionary fears plague the global economy and market turbulence becomes the norm, gold has been written about and discussed widely by experts in the financial media.

Today, just as always, gold and silver are a sensible way to shield your finances from cyber criminals.

If you’re ready to protect your family’s future from hackers by diversifying your retirement with “safe-haven” assets that are virtually impervious to cybercrime, call The Hartford Gold Group and speak to a gold and silver specialist right now. There is no obligation, and your one-on-one consultation is absolutely free: 800-888-8888
HERE ARE 11 OTHER CONCRETE STEPS TO FOLLOW TO MINIMIZE THE RISK OF BEING A CYBERCRIME VICTIM:

1. Don’t complete your social media file.
2. Be careful about sharing your Social Security number – even the last 4 digits.
3. Lock down your hardware.
4. Turn on private browsing.
5. Use a passcode vault that generates and remembers strong and unique passwords.
6. Use two-factor authentication.
7. Set up a Google alert on your own name.
10. Don’t give your zip code when making credit card purchases.
11. Lie when setting up password security questions.
The Hartford Gold Group (HGG) is a family-owned company in Los Angeles, CA that helps individuals and families diversify and protect their wealth with precious metals. Through our website, publications and expert Product Specialists, The Hartford Gold Group offers a wealth of precious metals market perspective that empowers both new and experienced investors.