

COUNTERING CYBERSCAMMING

A man in a dark suit is seen from behind, looking towards a large, stylized blue ribbon graphic. The ribbon is composed of several segments, each containing a different icon: a globe, a hand holding a globe, a person standing on a globe, a hand holding a globe, a globe with a grid, a hand holding a globe, a globe with a grid, and a hand holding a globe. The background is a light blue gradient with a grid pattern.

Nicole Foga
Foga Daley
Attorneys-at-law
September 30, 2013

COUNTERING CYBER SCAMMING



Establish a Legal Framework that criminalizes cyber scamming in particular and creates cyber crime offences in general.

COUNTERING CYBER SCAMMING

In 2010 the Cybercrimes Act was passed

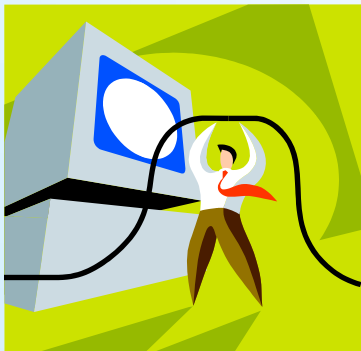
On March 28, 2013

**The Law Reform (Fraudulent Transactions)
(Special Provisions) Act**

COUNTERING CYBER SCAMMING



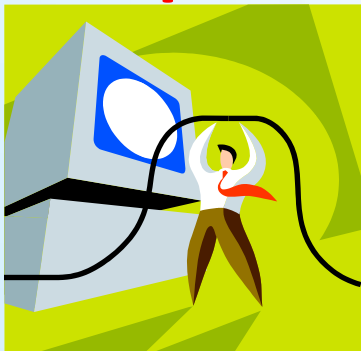
Recognize that once you have a business and a computer/mobile device which connects to the internet you are at risk and cybersecurity issues are relevant to you.



COUNTERING CYBER SCAMMING



KNOWLEDGE IS POWER utilizing what you know is Empowerment **FAILING** to address cybersecurity issues may be Negligent, irresponsible and criminally reckless .



COUNTERING CYBER SCAMMING

KNOW YOUR ENEMY

What is a scammer/cyber criminal after:

- **Money**
- **Data/Control**
- **Disruption/Chaos**



COUNTERING CYBER SCAMMING

CONDUCT A CYBER AUDIT OF YOUR BUSINESS



COUNTERING CYBER SCAMMING



**THE WORKPLACE CAN BE A
PLAYGROUND FOR CYBER SCAMMERS
AND CYBERCRIMINALS IN GENERAL**



Business in the 21st Century

Employers and Employees :

- *Use Smartphones – iPhone/Galaxy 6*
- *Receive and Respond to E-Mails*
- *Often engage in Social Media*
- *Create Digital Footprints*



Business Vulnerability

The failure of a Business to to identify, assess, and control vulnerabilities and threats and respond in a timely fashion



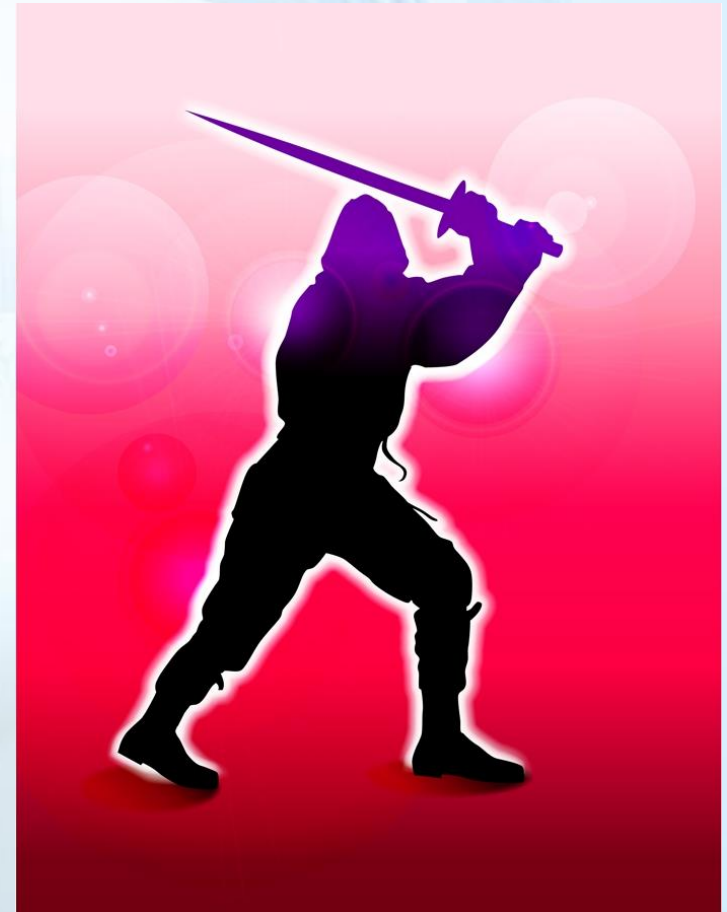
can result in economic loss, embarrassment and possible criminal conviction by aiding and abetting an offence.

Counter Business Vulnerability

Must be Mindful that:

Digital solutions are often twin edge swords.

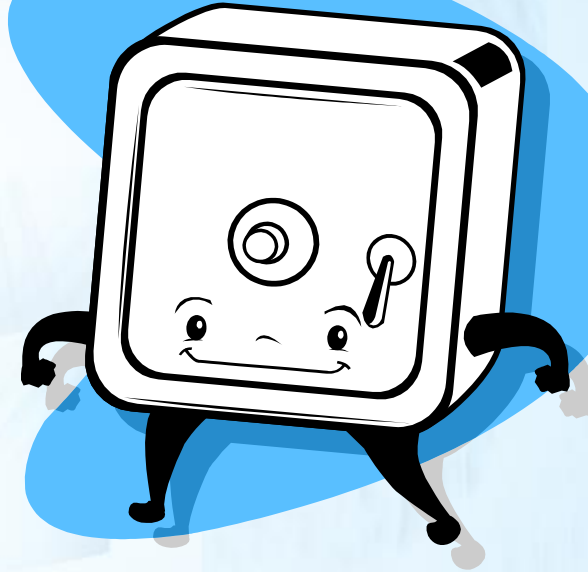
- *Tantalizing speed and efficiency of technology must be balanced with trust and confidentiality issues.*



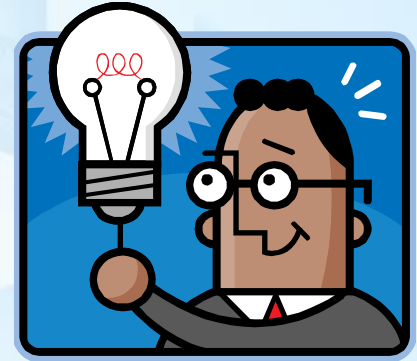
Countering Cyberscamming

What steps are taken to ensure that the information is secure?

Are sensitive files encrypted and/or password protected?



Counter Business Vulnerability



**DEVELOP AN INFORMATION
SECURITY PLAN**



Business Vulnerability

Businesses now routinely

• *Store sensitive clients/customer/supplier information in digital format on:*

- *office computers*
- *home computers,*
- *Laptops*
- *Smartphones*
- *Tablets*



Business Vulnerability

Must be Mindful of:

- *Malware*
- *Man-in-the-Middle attack*
- *Password Sniffing*
- *Phishing*
- *Pharming.*



Business Vulnerability

Must be Mindful of:

- *Shoulder Surfing*
- *Skimming*
- *Spoofing*
- *Spyware*
- *Trojan Horses*
- *Vishing*
- *Worms*



Business Vulnerability



Business Vulnerability

BE ALERT

BE ALERT



COUNTERING CYBERSCAMMING

SCAMS TARGETTING BUSINESSES

***Cheque Fraud –Solicitation
online***

***Phishing Enquiries - It is said that
if you teach someone to Phish they can feed
themselves forever***

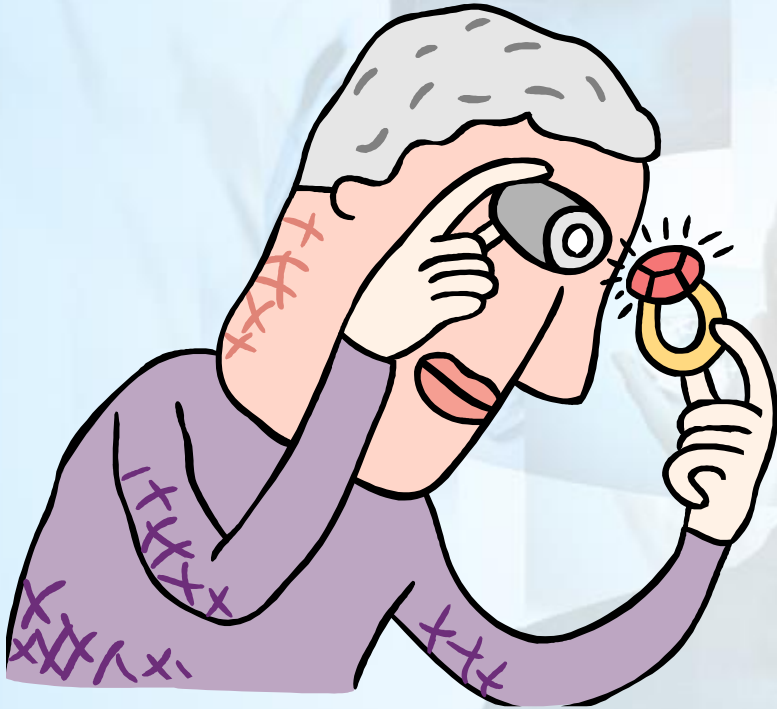
Business Vulnerabilities

TIPS - AVOIDING ONLINE SCAMS

1. Carefully scrutinize unsolicited email/phone calls from individuals or entities with whom you have no prior dealings requesting your services, particularly if the email/phone calls originate from a foreign country.



Business Vulnerabilities



TIPS - AVOIDING ONLINE SCAMS

- 2. VERIFY: the identify of the “client/customer” .
VERIFY: the information provided by the potential “client” “customer” “supplier” including the accuracy and genuineness of the information contained in the solicitation eg. phone numbers and addresses.*

Business Vulnerabilities

TIPS - AVOIDING ONLINE SCAMS

3. *The presence of numerous typos and/or variations of well known business is often a hint that the solicitation is not bona fide.*



Business Vulnerabilities

TIPS - AVOIDING ONLINE SCAMS

- 4. Be suspicious of a solicitation that offers a relatively large fees or commission for little or no work or that appears outside of your organizations area of core competences.*



Business Vulnerabilities

TIPS - AVOIDING ONLINE SCAMS

- 5. Don't jump the gun. Wait until the confirmation is obtained from the bank that the monies deposited have been cleared in accordance with bank policy*



Business Vulnerabilities

TIPS - AVOIDING ONLINE SCAMS

- 6. Educate your staff to be on the lookout for these types of schemes.*
- 7 Use Available Resources Online – plethora of Cybersecurity information*

CONCLUSION



**Attend and Participate in
More of
These Conferences!**



Thank you!

