PRESENTATION ON CYBER JAGROOKTA DIWAS

SUMIT KUMAR GUPTA, PGT Comp. Sc.

Kendriya Vidyalaya, Ambikapur

Cyber risk

Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems.

Cyber risk could materialize in a variety of ways, such as:

- Deliberate and unauthorized breaches of security to gain access to information systems.
- Unintentional or accidental breaches of security.
- Operational IT risks due to factors such as poor system integrity.

How cybercrime targets businesses

1. Staff shortcomings can leave you vulnerable. Cyber criminals can come from anywhere – and they could be closer than you think. More company employees are carrying out cyber attacks, and given their access to sensitive information, they have the ability to cause significant damage.

2. Cloud computing challenges security. The workforce is more mobile than ever, and when operations move off-site, traditional security measures will fall short.

3. Ransomware can infiltrate networks. Whether or not your business is connected to the cloud, ransomware is a serious threat that can quickly derail your operations.

Tips to help reduce risk of cyber attacks –

1. **Educate employees.** In today's workplace, security awareness training isn't a luxury – it's a necessity. Take the time to teach employees:

- How to recognize cyber threats.
- How cyber attacks operate.
- How to react in case of a cyber attack.

2. **Segment networks -** Manage user privileges to ensure only authorized employees are able to access certain data sets, and remember to communicate any changes you make to the network.

3. **Update software.** Keep all software up to date so there are fewer weaknesses for criminals to exploit. It's important that you apply patches and other software fixes as they become available.

4. **Invest in a good defense system.** Apply an in depth approach to the IT system. Using multiple layers of security controls – firewall, intrusion prevention system (IPS), and intrusion defense system (IDS)

The internet can be a dangerous neighborhood for everyone, but children and teens are especially vulnerable.
From cyber predators to social media posts that can come back to haunt them later in life, online hazards can have severe, costly, even tragic, consequences.
Children may unwittingly expose their families to internet threats, for example, by accidentally downloading malware that could give cyber criminals access to their parents' bank account or other sensitive information.

1. **Cyberbullying -** Children can be ridiculed in social media exchanges. Or, in online gaming, their player personas can be subjected to incessant attack, turning the game from an imaginative adventure into a humiliating ordeal that escalate into cyber bullying across multiple platforms and in real-life.

2. **Cyber Predators** These days sexual and other predators often stalk children on the internet, taking advantage of their innocence, lack of adult supervision and abusing their trust. This can culminate in children being lured into dangerous personal encounters IRL.

3. **Posting Private Information** Children do not yet understand social boundaries. They may post personally identifiable information (PII) online, for example in their social media profiles, that should not be out in public. This might be anything from images of awkward personal moments to their home addresses or family vacation plans.

4. **Phishing -** Phishing is what cyber security professionals call the use of emails that try to trick people into clicking on malicious links or attachments. These can be especially difficult for kids to detect because often, the email will appear to be from someone legitimate.

5. **Accidentally Downloading Malware -** Malware is computer software that is installed without the knowledge of permission of the victim and performs harmful actions on the computer. This includes stealing personal information from your computer or hijacking it for use in a "botnet,“ which causes sluggish performance.

BE CAUTIOUS

Do not share personal information like name, date of birth, address, phone number on online gaming sites/apps

- Never share your or your parent's credit/debit card details
- Never install games from free online gaming websites
- Never download games from links received in email or SMS
- Never download/install pirated games and software

Never share any of your passwords; change passwords frequently

- Install good antivirus software on your computer/smartphone
- Cyber criminals might try to befriend you; they have wrong intentions
- Never use voice chat or web cam while playing online
- Never meet in person someone from the online gaming world

Cyber risks due to online gaming –

1. Phishing

The same tactics scammers use to trick people out of their credit card numbers, bank passwords, and other account logins are also popular with gaming thieves. In this case, instead of mocking up a replica of Chase Bank or the like, criminals may build something that looks like a popular online game website and urge gamers to change their password or validate their account, typically threatening to block the gamer's account unless they comply. The goal is to take over the account and resell it on the black market.

Solution: Phishing is phishing. Never click a link in an e-mail or text message. Open your Web browser, type in the game website yourself, log in to your account, and perform any checks or confirmations there. Use online protection that prevents your browser from opening fake sites.

2. Trolls and bullying

Almost every online game includes some form of voice or text-based chatting nowadays. Unfortunately, the feature is also widely abused. In the heat of the online battle, you may hear some cursing, or an insult. That may just be human nature in a highly competitive atmosphere, but inevitably, some players will cross the line into bullying other players.

Solution: Immediately block any offender; don't play or chat with them, and report their user name to the game abuse team.

3. Cheats and frauds

Depending on the rules and the type of game, multiple ways to cheat may exist — some considered legitimate, some not. The worst use modified gaming clients, or even bots, to play in better condition (with greater speed or precision, for example) than ordinary players.

Solution: Don't accept suspicious offers from strangers. If an offer sounds too good to be true, it probably is. If you notice someone progressing too fast in the game, report it to the support team.

4. Character and inventory theft

Criminals are likely to target in-game resources, well-developed game characters, paid game accounts, or associated credit-card data. The latter is the hardest to target, but others may be stolen from you in multiple ways: phishing, password-stealing malware, in-game fraud and so on.

Solution: As you progress in a game, be more and more cautious with your account. Set up two-factor authentication for the account, use complex and unique passwords for your in-game account and your primary e-mail address, use a strong security solution for your device, and watch out for phishing and other attempts to steal your credentials.

5. Computer or smartphone compromise

In addition to other tricks that work for a general audience, some hackers target gamers with fake game updates or utilities claiming to customize your game or help speed your game progress. Malicious apps spread through phishing, in-game communications, as attachments on gamers' forums or chat rooms, and by other, similar means.

Solution: The aforementioned malware is why gamers always need fully updated devices with the most recent patches from OS vendors and the strongest Internet security suite available. Some solutions, such as Kaspersky Internet Security, protect you from malware and phishing and also include a special gaming mode, which delays or disables certain features so your security won't cause any computer slowdowns while you're kicking butt online.

Game security solutions

Alibaba Cloud Security - Game Service

Anti-DDoS IP Address

- Protection peak bandwidth of 20 - 300 Gbps, and the protection threshold can be elastically adjusted
- Services available on a 7*24 basis to support major activities

Game Shield

- Defense against DDoS, CC and web vulnerability attacks
- BGP bandwidth access, cross-operator and nearby access
- Joint-action mechanism with Anti-DDoS IP attack defense service in traffic flooding attacks

Mobile security

- App risk scan and counterfeit monitoring
- App security reinforce and security components

Data risk control

- Anti-spam registration and anti-credential stuffing attacks and account theft
- Anti-traffic cheating

Security management

- RAM resource access control to avoid account sharing and loose permissions
- Configuration of security group firewall policies to implement security access control
- VPN+bastion hosts to secure access and log all actions
- The precognition plan to protect system and interface security
- On-cloud security management center

Every year, we lose millions of rupees to the activities of scammers who bombard us with online, mail, door-to-door and telephone scams.

SCAMMERS DO NOT DISCRIMINATE

Scammers target people of all backgrounds, ages and income levels. Fake lotteries, Internet frauds, get-rich-quick schemes and miracle health cures are some of the favoured means of separating the unwary from their money. New varieties of these scams appear all the time.

The Competition Bureau has seen the devastating effects scams can have on people and their families. One of the best ways to combat this kind of fraud is to take measures to prevent yourself from being caught in the first place.

LOTTERIES, SWEEPSTAKES AND CONTESTS

WHAT TO LOOK FOR

You cannot win money or a prize in a lottery unless you have entered it yourself, or someone else has entered it on your behalf. You cannot be chosen as a random winner if you don't have an entry. Many lottery scams try to trick you into providing your banking and personal details to claim your prize. You should not have to pay any fee or tax to claim a legitimate prize. Don't be fooled by claims that the offer is legal or has government approval—many scammers will tell you this. Instead of receiving a grand prize or fortune, you will lose every cent that you send to a scammer. And if you have provided other personal details, your identity could be misused too.

A fake prize scam will tell you that you have won a prize or a contest. You may receive a phone call, an email, a text message or see a pop-up screen on your computer. There are often costs involved with claiming your prize, and even if you do receive a prize, it may not be what was promised to you.

The scammers make their money by making you pay fees or taxes, call their premium rate phone numbers or send premium text messages to claim your prize. These premium rate calls can be very expensive, and the scammers will try to keep you on the line for a long time or ask you to call a different premium rate number.

!	PROTECT YOURSELF
REMEMBER	Legitimate lotteries do not require you to pay a fee or tax to collect winnings.
CAUTION	Never send money to anybody you don't know and trust.
THINK	Don't provide personal banking details to anyone that you do not know and trust.
INVESTIGATE	Examine all of the terms and conditions of any offer very carefully—claims of free or very cheap offers often have hidden costs. Calls to premium rate phone numbers or premium text messages can be very expensive.
ASK YOURSELF	Did I enter this contest? You cannot win money or a prize in a contest unless you have entered it yourself, or someone else has entered it on your behalf.

PYRAMID SCHEMES

Pyramid schemes promise a large financial return for a relatively small cost.
Pyramid schemes are illegal and very risky—and can cost you a lot of money.

!	PROTECT YOURSELF
REMEMBER	Pyramid and Ponzi schemes may be sent to you from family members and people you trust—they might not know that they could be illegal or that they are involved in a scam.
CAUTION	Never commit to anything at high-pressure meetings or seminars.
THINK	Don't make any decisions without doing your homework—research the offer being made and seek independent advice before making a decision.
INVESTIGATE	Do some research on all business opportunities that interest you.
ASK YOURSELF	If I am not selling a genuine product or service, is participation in this activity legal?

MONEY TRANSFER REQUESTS

Money transfer scams are on the rise. Be very careful when someone offers you money to help transfer their funds. Once you send money to someone, it can be very difficult, if not impossible, to get it back.

!	PROTECT YOURSELF
REMEMBER	If you have been approached by someone asking you to transfer money for them, it is probably a scam.
CAUTION	Never send money, or give credit card or online account details to anyone you do not know and trust.
THINK	Don't accept a cheque or money order for payment for goods that is more than what you agreed upon. Send it back and ask the buyer to send you payment for the agreed amount before you deliver the goods or services.
INVESTIGATE	Examine the information on the Canadian Anti-Fraud Centre website for information on how to protect yourself against money transfer scams.
ASK YOURSELF	Is it really safe to transfer money for someone I do not know?

INTERNET SCAMS

A lot of Internet scams take place without the victim even noticing. You can greatly reduce the chances of being scammed on the Internet if you follow some simple precautions.

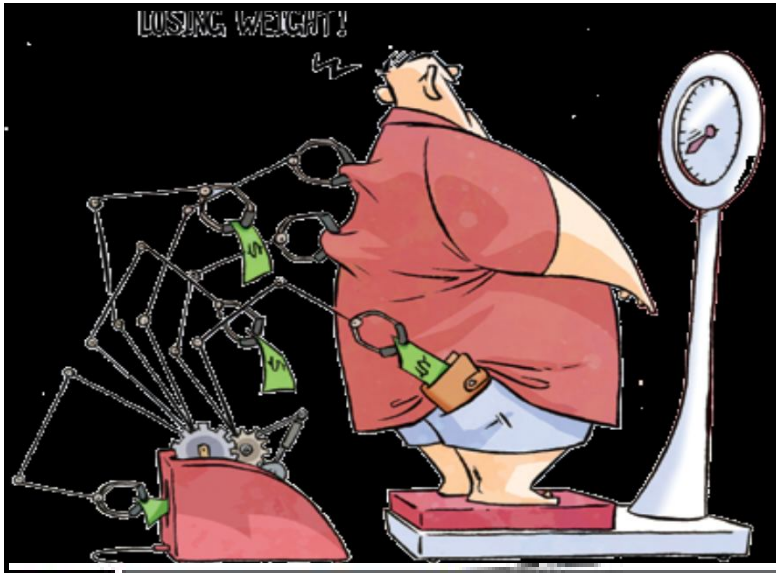
!	PROTECT YOURSELF
REMEMBER	If you choose to shop online or participate in online auctions, make sure you know about refund policies and dispute-handling processes, and be careful that you are not overcharged. Also, you may want to use an escrow service, such as PayPal. This service will hold your payment and only release it to the seller once you have confirmed that you received what you paid for. There is usually a small fee for this service. A legitimate bank or financial institution will never ask you to click on a link in an email or send your account details through an email or website.
CAUTION	Never buy from bidders with poor ratings on auction sites, and do your best to ensure that you are only making purchases from genuine shopping sites. Never provide your personal, credit card or account information unless you are certain the site is genuine.
THINK	Don't reply to spam emails, even to unsubscribe, and do not click on any links or call any telephone number listed in a spam email. Make sure you have current protective software or get advice from a computer specialist.
INVESTIGATE	If an email or pop-up offers you a product or service that genuinely interests you and it seems reasonable, be sure that you understand all the terms and conditions and costs involved before making a purchase or providing your details.
ASK YOURSELF	By opening this suspect email, will I risk the security of my computer? Are the contact details provided in the email correct? Telephone your bank or financial institution to ask whether the email you received is genuine.

MOBILE PHONE SCAMS

Mobile phone scams can be difficult to recognize.
Be wary of somebody who talks as if they know you or of redialing a missed call from an unknown number—there may be hidden charges.

! PROTECT YOURSELF

REMEMBER	Text "STOP" to end unwanted text messages or to end unwanted subscriptions.
CAUTION	Never reply to text messages offering you free ringtones or missed calls from numbers that you do not recognize.
THINK	Don't call or text phone numbers beginning with 1-900 unless you are aware of the cost involved, and carefully read any terms and conditions when texting short codes.
INVESTIGATE	Read all the terms and conditions of an offer very carefully. Services offering free or very cheap products often have hidden costs.
ASK YOURSELF	Do I know how to stop any subscription service I want to sign up to?



HEALTH AND MEDICAL SCAMS

Medical scams prey on human suffering. They offer solutions where none exist or promise to simplify complex health treatments.

! PROTECT YOURSELF

REMEMBER	There are no magic pills, miracle cures or safe options for serious medical conditions or rapid weight loss.
CAUTION	Never commit to anything under pressure.
THINK	Don't trust an unsubstantiated claim about medicines, supplements or other treatments. Consult your healthcare professional.
INVESTIGATE	Check for published medical and research papers to verify the accuracy of the claims made by the promoters.
ASK YOURSELF	If this really is a miracle cure, wouldn't my healthcare professional have told me about it?

EMERGENCY SCAMS

Emergency scams target grandparents and play upon their emotions to rob them of their money.

! PROTECT YOURSELF

REMEMBER	Scammers are counting on the fact that you will want to act quickly to help your loved ones in an emergency.
CAUTION	Never send money to anyone you don't know and trust. Verify the person's identity before you take any steps to help.
THINK	Don't give out any personal information to the caller.
INVESTIGATE	Ask the person questions that only your loved one would be able to answer. Call the child's parents or friends to verify the story.
ASK YOURSELF	Does the caller's story make sense?

DATING AND ROMANCE SCAMS

Despite the many legitimate dating websites operating in Canada, there are many dating and romance scams as well. Dating and romance scams try to lower your defenses by appealing to your romantic and compassionate side.

!	PROTECT YOURSELF
REMEMBER	Check website addresses carefully. Scammers often set up fake websites with very similar addresses to legitimate dating websites.
CAUTION	Never send money, or give credit card or online account details to anyone you do not know and trust.
THINK	Don't give out any personal information in an email or when you are chatting online.
INVESTIGATE	Make sure you only use legitimate and reputable dating websites.
ASK YOURSELF	Would someone I have never met really declare their love for me after only a few letters or emails?

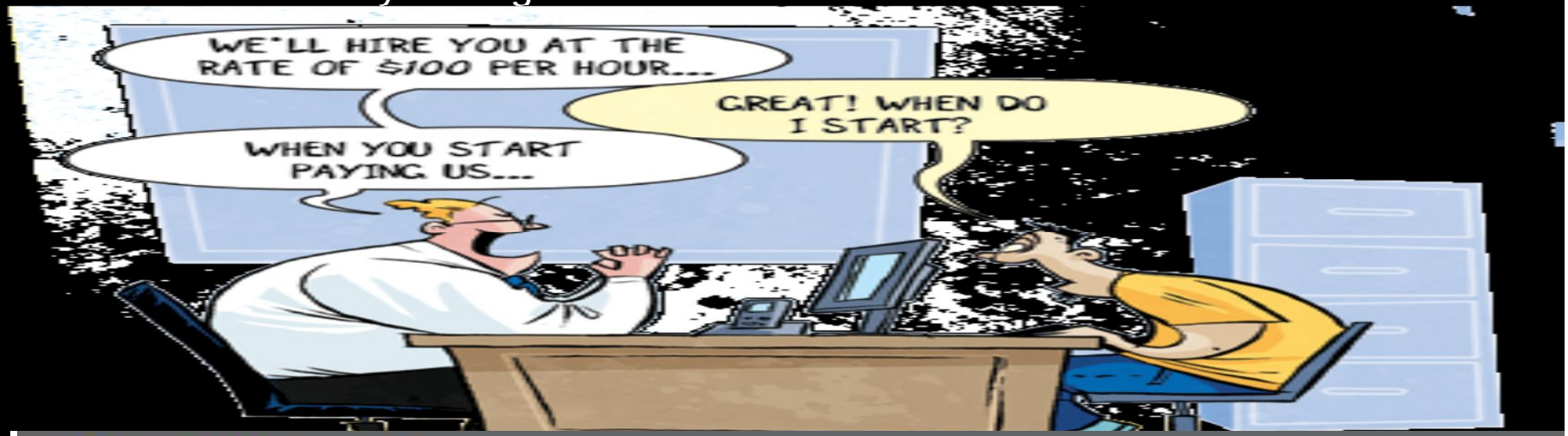
CHARITY SCAMS

Charity scams take advantage of people's generosity and kindness by asking for donations to a fake charity or by impersonating a real charity.

!	PROTECT YOURSELF
REMEMBER	If you have any doubts at all about the person asking for money, do not give them any cash, credit card or bank account details.
CAUTION	Never give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
THINK	If in doubt, approach an aid organization directly to make a donation or offer support.
INVESTIGATE	Search the Canada Revenue Agency database to check that the charity that has approached you is genuine.
ASK YOURSELF	How and to whom would I like to make a contribution?

JOB AND EMPLOYMENT SCAMS

Job and employment scams target people looking for a job. They often promise a lot of income—sometimes they even guarantee it—for little or no effort.



! PROTECT YOURSELF

REMEMBER	There are no shortcuts to wealth—the only people that make money are the scammers.
CAUTION	Never send your bank account or credit card details to anybody you do not know and trust. If you cash the cheque and it turns out to be counterfeit, you could be held accountable for the entire monetary loss by your bank.
THINK	Don't make any decisions without carefully researching the offer. Seek independent advice before making a decision.
INVESTIGATE	Beware of products or schemes claiming to guarantee income and job offers requiring payment of an upfront fee or sending money through a money transfer service. Make sure any franchise business opportunity is legitimate.
ASK YOURSELF	Did I get all the details in writing before paying or signing anything?

SMALL BUSINESS SCAMS

Scams that target small businesses can come in a variety of forms—from bills for advertising or directory listings that were never ordered to dubious office supply offers.

! PROTECT YOURSELF	
REMEMBER	Make sure that the people processing the invoices or answering telephone calls are aware of these scams. They will most often be the point of contact for the scammers. Always check that goods or services were both ordered and delivered before paying an invoice.
CAUTION	Never give out or update any information about your business unless you know what the information will be used for.
THINK	Don't agree to a business proposal over the phone—always ask for an offer in writing. Limit the number of people in your business that have access to funds and have the authority to approve purchases.
INVESTIGATE	Effective management procedures can go a long way towards preventing these scams from succeeding. Having clearly defined procedures for the verification, payment and management of accounts and invoices is an effective defence against these types of scams.
ASK YOURSELF	If a caller claims that I have ordered or authorized something and I do not think it sounds right, shouldn't I ask for proof?

SERVICE SCAMS

Many Canadians are being targeted by individuals claiming to offer reduced rates or deals for various services.

!	PROTECT YOURSELF
REMEMBER	Only your service provider can offer you a better rate or price for their services.
CAUTION	Be wary of unsolicited calls from people offering a great deal "for a limited time only".
THINK	Don't give out your credit card number over the phone unless you made the call and the number came from a trusted source.
INVESTIGATE	If a caller claims to represent your bank, telephone your bank to ask whether the offer you received is genuine.
ASK YOURSELF	By offering up this information, am I putting myself at risk?

HANDY HINTS TO PROTECT YOURSELF

PROTECT YOUR IDENTITY

• Only give out your personal details and information where it is absolutely necessary and when you trust the person you are speaking to or dealing with.

• Destroy personal information: don't just throw it out. You should cut up or shred old bills, statements or cards—for example, credit cards and ATM cards.

• Treat your personal details like you would treat money: don't leave them lying around for others to take.

MONEY MATTERS

• Never send money to anyone that you don't know and trust.

• Do not send any money or pay any fee to claim a prize or lottery winnings.

• "Jobs" asking you to simply use your own bank account to transfer money for somebody could be a front for money-laundering activity. Money laundering is a serious criminal offence.

• Avoid transferring or wiring any refunds or overpayments back to anyone you do not know.

THE FACE-TO-FACE APPROACH

• If someone comes to your door, ask to see some identification. You do not have to let them in, and they must leave if you ask them to.

• Before you decide to pay any money, if you are interested in what a door-to-door salesperson has to offer, take the time to find out about their business and their offer.

• Contact the Competition Bureau, provincial and territorial consumer affairs offices or the Better Business Bureau of your province or territory if you are unsure about a seller that comes to your door. See pages 29 and 30 for contact information.

HANDY HINTS TO PROTECT YOURSELF

TELEPHONE BUSINESS

• If you receive a phone call from someone you do not know, always ask for the name of the person you are speaking to and who they represent. Verify this information by calling the company yourself.
• Do not give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
• It is best not to respond to text messages or missed calls that come from numbers you do not recognize. Be especially wary of phone numbers beginning with 1-900. These may be charged at a higher rate than other numbers and can be very expensiv

EMAIL OFFERS

• Never reply to a spam email, even to unsubscribe— often, this just serves to “verify” your address to scammers. The best course of action is to delete any suspicious emails without opening them.
• Turn off the “viewing pane” as just viewing the email may send a verification notice to the sender that yours is a valid email address.
• Legitimate banks and financial institutions will never ask you for your account details in an email or ask you to click on a link in an email to access your account.
• Never call a telephone number or trust other contact details that you see in a spam email.

HANDY HINTS TO PROTECT YOURSELF

INTERNET BUSINESS

• Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.

• If you want to access a website, use a bookmarked link to the website or type the address of the website into the browser yourself. Never follow a link in an email.

• Check website addresses carefully. Scammers often set up fake websites with addresses very similar to legitimate websites.

• Beware of websites offering “free” downloads (such as music, adult content, games and movies). Downloading these products may install harmful programs onto your computer without you knowing.

• Avoid clicking on pop-up ads—this could lead to harmful programs being installed on your computer.

• Never enter your personal, credit card or online account information on a website that you are not sure is genuine.

HANDY HINTS TO PROTECT YOURSELF

INTERNET BUSINESS

• Never enter your personal, credit card or online account information on a website that you are not sure is genuine.

• Never send your personal, credit card or online banking details through an email.

• Avoid using public computers (at libraries or Internet cafes) to do your Internet banking or online shopping.

• When using public computers, clear the history and cache of the computer when you finish your session.

• Be careful when using software on your computer that auto-completes online forms. This can give Internet scammers easy access to your personal and credit card details.

• Choose passwords that would be difficult for anyone else to guess—for example, passwords that include letters and numbers. You should also regularly change passwords.

• When buying anything online, print out copies of all transactions and only pay via a secure site. If using an Internet auction site, note the ID numbers involved andread all the security advice on the site first

SCAMS AND YOU:
WHAT TO DO IF YOU GET SCAMMED!

Authorities may not always be able to take action against scams, even if it seems like a scammer might have broken the law.

REDUCING THE DAMAGE

- If you have been tricked into signing a contract or buying a product or service
- If you think someone has gained access to your online account, telephone banking account or credit card details
- If the scam relates to your health
- If you have sent money to someone that you think may be a scammer
- If you have been tricked by a door-to-door seller
- If you have been scammed using your computer
- If the scam involves yourmobile phone

GETTING HELP AND REPORTING A SCAM

The best agency to contact depends on where you live and what type of scam is involved.

If you think you have spotted a scam or have been targeted by a scam, there are a number of government and law enforcement agencies in Canada that you can contact for advice or to make a report. This may help you and prevent others from being ripped off by scam operators.

LOCAL SCAMS : Contact your local consumer affairs office

FINANCIAL AND INVESTMENT SCAMS : Contact Canadian Securities Administrators

REPORTING BANKING AND CREDIT CARD SCAMS : Contact your bank or financial institution

REPORTING SPAM EMAILS AND SMS

REPORTING FRAUD, THEFT AND OTHER CRIMES : Contact the police

CYBER JAGROOKTA DIWAS

THANK YOU

KENDRIYA VIDYALAYA, AMBIKAPUR

Kendriya Vidyalaya, ambiKapur