Cyber Security in Consumer Business

Consumer privacy, also known as customer privacy, involves the handling and protection of the sensitive personal information provided by customers during everyday transactions. The internet has evolved into a medium of commerce, making consumer data privacy a growing concern. Despite the proliferation of connected devices and the personal information and sensitive data they harbour, many consumers are unaware of just how susceptible they are to cyber attack. In fact, some of the most severe cyber security threats originate from a lack of consumer awareness, especially when it comes to securing personal data.

For today's businesses, harnessing emerging technologies in order to redefine products, services, and consumer experiences is often the new cost of doing business. Technology investment, however, can drive more than just profit potential. Widespread initiatives around customer analytics, cloud integration, connected devices, and digital payment technology are likely leaving businesses increasingly exposed to cyber threats. Some threats, such as credit card fraud and identity theft, are becoming all too familiar in today's marketplace and can be significantly detrimental to customer trust and brand reputation.

The CPA (Consumer Protection Act 2007) requires traders to be transparent and places a wide range of responsibilities on traders. Under the CPA it is a criminal offence for any retailer to make a false or misleading claim about goods, services and prices. It is also an offence to sell goods which bear a false or misleading description. The CPA protects consumers from misleading, aggressive or prohibited practices. In other words, when a breach of good faith occurs, and the consumer is denied the reasonable standard of skill and care which they are entitled to. A misleading practice involves providing false, misleading and deceptive information. Misleading advertising, misleading information and withholding material information are considered misleading practices.

What should Consumers do

Stop using public computers/ cyber cafes for office work.

When on tour, don't avail such services that require location information.

Do not click on untrusted links even if they appear to be from a legitimate source. For example, any link to a cricket score website on an airline ticket booking page.

Don't perform any financial transactions by using public computers or public Wi-Fi connections. There is a risk that your information can be read by unauthorized people.

Be careful while entering passwords in front of others. Change your password immediately if you suspect that it has been compromised.

Avoid disclosing/ sharing any official information on untrusted phone calls, meetings or email messages. Attackers often pose as genuine people to gain confidential official information to cause a data breach.

Always look for a green/grey padlocked symbol of "https".

You may see the yellow warning triangle and the lock icon in the address bar while visiting a webpage that's secured with SSL. This means that the website use non-secured third-party resources, like scripts or images. ***Do not send any sensitive information to sites where the Site Identity button is a gray padlock with a yellow warning triangle.***

For Google Chrome, it is an indication that the browser had found insecure content on that page, either because the page contains both HTTPS and HTTP content, or because the browser detected that the website is using an obsolete encryption mechanism, such as SHA-1.

For Firefox, A gray padlock with a yellow warning triangle indicates that the connection between Firefox and the website is only partially encrypted and doesn't prevent eavesdropping. By default, Firefox does not block insecure passive content such as images; you will simply see a warning that the page isn't fully secure.

Sometimes Firefox shows a gray padlock with a red strike-through line over it, when the user reaches an HTTP page that contains a username+password log-on combination. A padlock with a red strike over it indicates that the connection between Firefox and the website is either delivered using an insecure protocol (HTTP or FTP) or that it is only partially encrypted because you've manually deactivated mixed content blocking. The site doesn't prevent against eavesdropping or man-in-the-middle attacks. ***Do not send any sensitive information to sites where the Site Identity button is a gray padlock with a red strike over it.***

REF:

1. https://www.kinamo.be/en/support/faq/why-do-i-see-a-yellow-warning-triangle-on-an-https-secured-website#:~:text=The%20yellow%20warning%20triangle%20you,an%20obsolete%20encryption%20mechanism%2C%20such
2. https://support.gogetssl.com/index.php?/Knowledgebase/Article/View/39/0/yellow-padlock
3. https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure
4. https://www.computerworld.com/article/3275726/how-your-web-browser-tells-you-when-its-safe.html
5. https://pixabay.com