Cybersecurity for Small Businesses

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

SVC secure verify connect

CSB

CYBER SECURITY BRUNEI

BRUCERT

BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

NDFL

NATIONAL DIGITAL FORENSICS LABORATORY

CYBERWATCH CENTRE

Objectives

- Equip small business owners with essential knowledge and skills to protect their businesses from cyber threats.
- Raise awareness about common cyberattacks and their potential impact on small businesses.
- Provide practical tips and strategies to prevent cyberattacks and enhance cybersecurity measures.

Course Overview

- Introduction
- Latest Cyber Threats:
  - Social Media: Instagram Takeover
  - Bad Software: Ransomware
  - Social Engineering: Phishing
- Basic Cybersecurity Tips
- What can you report to BruCERT?

Introduction

Importance of cybersecurity awareness

Importance of Cybersecurity Awareness

95%

Data breaches are caused by human error

Source:
IBM Cyber Security Intelligence Index Report.

Importance of cybersecurity for small businesses

- Cyberattacks result in financial losses, reputation damage, legal consequences, and business distruption
- Cybersecurity safeguard critical information.
- Implementing measures for trust and compliance.

Impact of cyberattacks

- Financial loss
- Reputational damage
- Operation distruption
- Legal consequences - for more info kindly refer to:
  - Cyber Security Order, 2023 (link)
  - Personal Data Protection (link)

Latest Cyber Threats

Latest Cyber Threats

- Social Media: Instagram takeover
- Bad Software: Ransomware
- Social Engineering: Phishing

Social Media:

Instagram Takeover

Small businesses on Instagram

In Brunei Darussalam, many people use Instagram to sell or showcase their products online. This is because Brunei has a high number of active social media users globally. Even though Instagram isn't designed for buying and selling, people in Brunei often use it for this purpose. However, there are drawbacks, such as scams.

Pros & Cons of selling on Instagram

Pros	Cons
Visual appeal: Instagram provides a visually engaging platform, allowing sellers to showcase products effectively through images and videos.	Limited Security: Transactions on Instagram may lack the same level of security as dedicated ecommerce platforms, potentially exposing buyers to scams or fraud.
Direct Interaction: Sellers can directly interact with buyers.	Transaction Risks: Some buyers may fail to pay or ghost the seller
Discoverability: Users can easily discover new and unique products through features like Explore, hashtags, and sponsored posts.	Lack of Regulation: Compared to dedicated ecommerce platforms, Instagram transactions may lack regulatory oversight, making dispute resolution more complex.

Hacked Instagram Business Account

Case Study

- Users receive deceptive WhatsApp messages, purportedly from Instagram, alleging copyright issues and prompting them to share account credentials through a fake Objection Form.
- Hijackers demand ransom after compromising account.
- It is important to enable two-factor authentication for account recovery.

For more info:
https://www.secureverifyconnect.info/hacked-business-instagram-account


ADVISORY

HACKED BUSINESS INSTAGRAM ACCOUNT

BruCERT has received an alarming number of reports from users whose Instagram account has been taken over, with a demand for ransom to be paid in order to regain access to their account. The main targets are Instagram business accounts or personal accounts with many followers and their contact number in their profile.

First, the user receives a WhatsApp message from a foreign number claiming to be from Instagram, informing them of copyright infringement complaints from other Instagram users. The message also contains a link to an Objection Form, where the user is required to provide their business Instagram username and password. After submitting their credentials, the user's Instagram account will be compromised, and they will be asked to pay a ransom.

Research shows that users who have not enabled two-factor authentication are unlikely to regain control of their account.

1 of 4 | 06 October 2022

CSB CYBER SECURITY BRUNEI

BRUCERT BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

Pros & Cons of using Tracking Devices

Pros	Cons
Can be used to track valuables	Some tracking devices rely on other users' devices (in close proximity) in order to pinpoint their exact location.
Can be used to track lost or stolen items	There is a risk that the tracker can be used for malicious intent such as stalking, harassment or tracking someone without their consent.
Able to track a child or elderly person's location for safety purposes	Tracking devices can be exposed to cyberattacks hence it is important to update with the latest security patches.

Best Practices

Instagram

- Enable two-step verification for social media, email, and other important accounts.
- Click links with caution. Social media accounts are regularly hacked. Never click on any links received from an unknown sender.
- When receiving an unexpected message, take some time to think about the legitimacy of the message. Look out for language or content that does not sound right. Notices from Instagram would most likely be sent as a notification through Instagram or email, not WhatsApp.

Best Practices

Instagram

- Keep an eye on your Instagram login activity and monitor the list of devices currently logged into your account. Settings > Security > Login Activity
- Be aware of fake Instagram notifications. Instagram has a helpful feature called "Emails from Instagram" that lets you see any communications the company sends to you. Use this feature every time you think someone is trying to get into your account by sending you emails pretending to be from Instagram. Settings > Security > Emails from Instagram

Best Practices

Instagram

- If your credentials have been compromised, reset your password. Create a strong password with a minimum of 10 characters and a combination of letters, numbers, and special characters, or use a passphrase. Change your password every 3-6 months.
- Use a different password for each of your accounts.
- Limit the sharing of personal information (e.g., full name, birthdate, address, phone number) on social media as an attacker can take advantage of your personal details.

Best Practices

Instagram

- Take time to browse all the privacy settings and control who can see your profile, past posts, and future posts. Make sure your phone number and email address are hidden from public view.
- Familiarize yourself with the privacy policies of the social media channels you use.
- Protect your computer and devices by installing antivirus software and set it to update automatically.

Bad Software:

Ransomware

Ransomware

Ransom Software

Ransomware is designed to block access to a computer system until a sum of money is paid.

Example of ransomware

Encryption: Ransomware encrypts files on the victim's computer, making them inaccessible. Decryption keys are then offered in exchange for the ransom payment.

Anonymous Communication: Ransomware attackers often communicate with victims through anonymous channels, such as email or Tor networks, making it challenging to trace or identify them.

Payment Instructions: Clear instructions on how to pay the ransom are provided, guiding victims through the process of acquiring and sending the cryptocurrency to the specified address.

Ransom Note: A ransom note is usually displayed on the victim's screen, explaining the situation, detailing the payment process, and issuing threats or consequences for non-compliance.

How can you get ransomware?

Downloads

Spam e-mail attachments

Malicious websites

Through file sharing programs

Best Practices

Protect yourself against ransomware

- Regularly backup your files and keep them at a separate storage
- Update your operating system and software
- Install and update reliable antivirus and anti-malware programs.
- Avoid opening attachments or links from unknown or suspicious emails.
- Stay updated on the latest cybersecurity threats and best practices.

Social Engineering:

Phishing

What is social engineering?

Social engineering is a way that some people use tricks or manipulation to get information from a victim by pretending to be someone they're not or by using psychological tactics. The information extracted from victims are usually used for fraudulent purposes. The most popular social engineering tactic now is phishing.

Common Forms of Social Engineering

Phishing

Stealing your information through e-mail, social media inbox
or website

Vishing

Stealing your information through telephone or voice call

Smishing

Stealing your information through SMS or instant messaging

Quishing

Stealing your information through QR code scanning

Phishing

In a phishing attack, the hacker tricks users into clicking a malicious URL that redirects them to a harmful website that either downloads harmful software or tries to get their private information.

How does Phishing work?

The victim clicks on a malicious link

The victim is directed to a phishing website.

The victim enters personal information such as login credentials into the fraudulent website.

Risks of phishing attacks

Identity theft

Financial fraud

Unauthorized access

Risks of phishing attacks

Data leak

Spread of malicious links

Malware breaches

Basic Cybersecurity Tips

Protect Yourself!

Basic Cyber Security Tips

- Install and update antivirus software regularly.
- Download software from trusted sources.
- Avoid suspicious links and check URLs before clicking.
- Never reuse passwords.
- Verify the identity of individuals you communicate with.
- Enable two-factor authentication (2FA).

Basic Cyber Security Tips

- Keep your OS and software up to date.
- Use secure, encrypted Wi-Fi connections.
- Back up your data regularly.
- Stay informed about common cybersecurity threats.
- Be cautious about sharing personal information on social media.
- Secure your mobile devices with passcodes or biometric locks.

What can you report to BruCERT?

What can you report to BruCERT?

Infected computer

Malicious website

Hacked email account

What can you report to BruCERT?

Phishing

Business Email Compromise

Social Media Threats

What can you report to BruCERT?

Website Defacement

Cyberbullying

Denial of Service

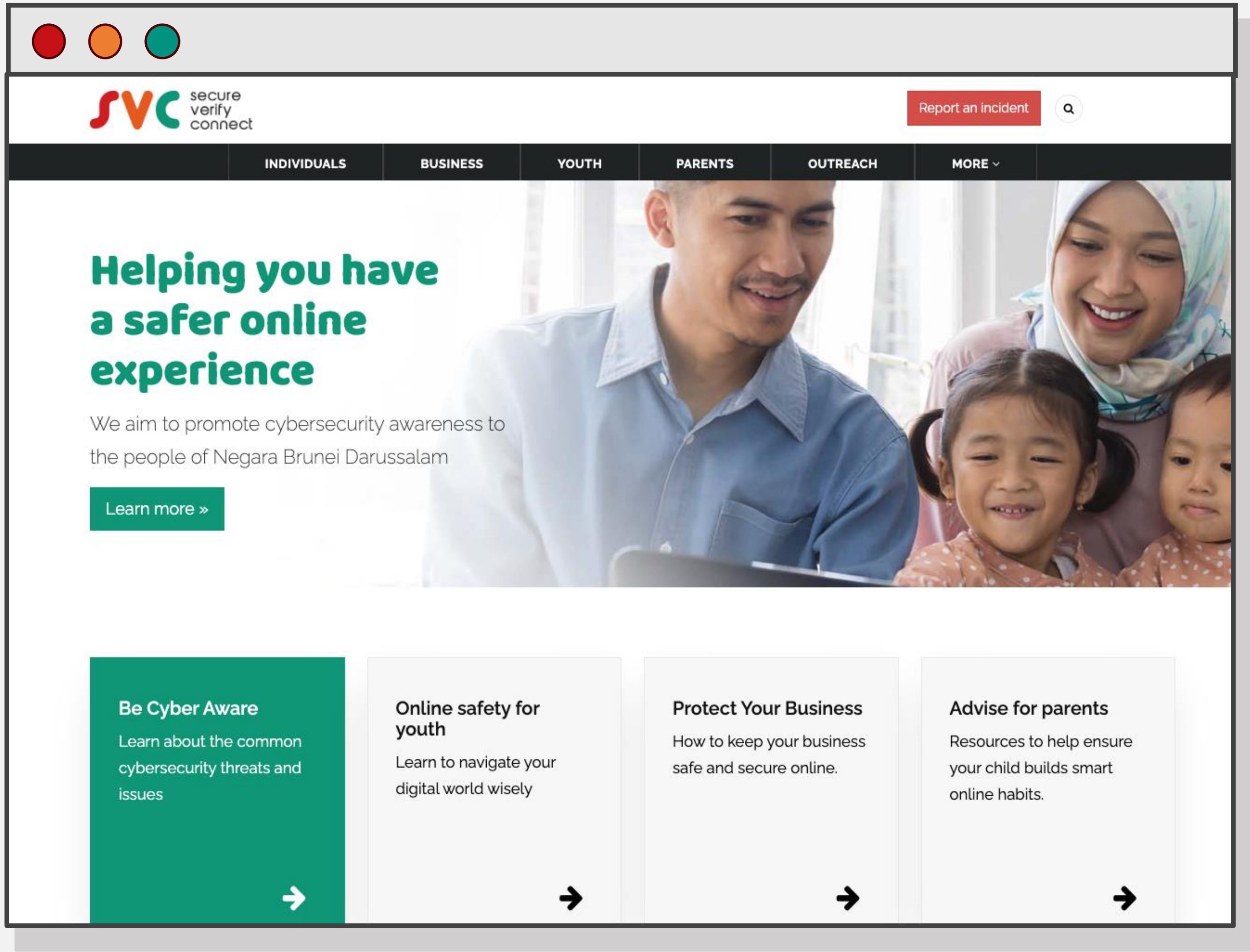
Report a Cybersecurity Incident

reporting@brucert.org.bn

245 8001

717 0766

www.SecureVerifyConnect.info



THANK YOU

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

@bruneicert

A TEAM UNDER

CSB
CYBER SECURITY BRUNEI