



Cyber Secure Education Campaign – Awareness Posters

February 2024



ARE YOU CYBER SECURE?



Use **COMPLEX** passwords



Ensure software is **UP TO DATE**



Be **CAREFUL** with removable media such as **USBs, CDs, and SD cards**



Follow the **SIG INTERNET ACCESS POLICY**



Don't click on **SUSPICIOUS** email links or attachments



Be **AWARE** of physical security



For more information:

helpdesk@sig.gov.sb

(+677) 24580 / 27668 / 27667




UPDATING PASSWORDS




Passwords are the first line of defence against any unauthorised access. Passwords protect personal and official information, act as a digital bodyguard, and prevent loss of data. Weak passwords can give criminals access to sensitive data and information.




DO

 **DO** create different passwords for different accounts



 **DO** use uppercase, lowercase, numbers and symbols in your passwords



 **DO** use long passwords, at least 14 characters in length



DON'T



DON'T use common passwords, such as "Password" or "Password123"



DON'T use personal details in your passwords (i.e. birthday, relative's names)



DON'T share passwords across accounts, or with other people



POTENTIAL ATTACKS



Brute Force: Guessing all possible password combinations.



Password Spray: Using common or leaked passwords across different accounts.



Shoulder-surfing: Looking over your shoulder to see the password.

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667



APPLYING UPDATES

Applying updates to software and computers is important for maintaining secure operations.

Legacy Systems refer to systems that vendors no longer update with security patches. Without updates, these legacy systems will be vulnerable as they are no longer being fixed by the company.

Software updates fix existing issues and make sure these vulnerabilities are patched!



DO



DO enable auto updates on applications and computers



DO regularly check for updates



DON'T



DON'T ignore update prompts



DON'T use software that is no longer supported/being updated unless necessary



POTENTIAL IMPACTS



Malware infection



Ransomware attack



Data breach

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667

REMOVABLE MEDIA



Removable media refers to any type of storage device that can be removed from a computer while the system is running. This includes:



USBs



SD Cards



CDs



DO



DO think before using any removable media



DO classify removable media based on its contents



DO label removable media according to its classification



DO report any suspicious removable media that is found in SIG workplaces



DON'T



DON'T plug in removable media without knowing where it came from



DON'T transfer files from SIG hardware onto removable media without permission



DON'T use personal removable media with SIG hardware without permission



POTENTIAL IMPACTS



Malware infection



Ransomware attack



Data breach

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667

PHISHING



Phishing is a method of stealing confidential information. Phishing involves sending fraudulent emails or messages to a victim to trick them into providing confidential information.

Phishing can happen in multiple ways, including via **email, SMS, social media, instant messaging platforms** and **phone calls**.



DO



DO stop, read and assess any suspicious looking emails



DO delete suspicious emails and report them to SIG ICT Services



DO confirm an email sender's identity if needed, for example by calling them



DON'T



DON'T click on suspicious emails or links



DON'T share your credit card information over email



DON'T provide your credentials to anyone



DON'T reply to suspicious emails



POTENTIAL IMPACTS



Data Theft



Money Theft



Business Disruption



Malware infection



Reputational Damage

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667

10 TIPS TO DETECT & HANDLE PHISHING EMAIL



Email display names may not reflect real senders.

When assessing email authenticity, verify the email address as sender identities can be manipulated or sent from compromised accounts.



Look but don't click.

Inspect hyperlinks by hovering over them without clicking. If the displayed text seems odd, avoid clicking it.



Check for grammatical or spelling errors.

Be careful with emails containing poor grammar as phishers may use tools to check spelling, resulting in correctly spelled but nonsensical messages.



Consider the salutation.

Bad actors may use generic greetings like "Dear valued customer" or omit greetings in suspicious messages. While not always a scam, these signs could indicate potential risks.



Is this email asking for personal information?

Be wary of emails asking for personal information; legitimate companies don't typically request it this way. When in doubt, contact the company directly or log in to your account on their website to confirm the request.



Be careful with attachments.

Be wary of email attachments, avoid opening suspicious ones, and verify with the sender if unsure. Watch out for official-looking attachments with hidden harmful links. Avoid HTM/HTML attachments as they can run code from your computer's memory.



Beware of urgency.

Be cautious of urgent emails that rush you into action. Phishing emails exploit trust and urgency to deceive recipients.



Check the email signature

Verify email signature to match sender's identity, preventing phishing scams with inconsistent signatures.



Don't believe everything you see.

If anything seems weird or not quite right, it's safer to be careful than to ignore it.



When in doubt, contact your SIG Helpdesk.

If you notice something unusual, contact your helpdesk via Servicely, Email, or phone to investigate and ensure safety.

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667

ACCEPTABLE USE



Acceptable use of government IT refers to the rules around what SIG employees can and cannot use their government issued devices for.

Government issued devices include desktop computers, laptops and any other devices provided by the Solomon Islands Government.



DO



DO think before you access websites for personal use



DO think before you open any files for personal use



DO read the SIG Internet Access Policy before you use government IT for personal use



DON'T



DON'T download files, including games, music or videos for personal use



DON'T access websites for personal use unless you know they are secure



POTENTIAL IMPACTS



Malware infection



Ransomware attack

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667

PHYSICAL SECURITY



Physical security aims to protect and keep people, property, physical assets and software safe from real-world threats and events or actions that cause damage. These threats can arise from internal or external intruders that interrogate data security.



DO



DO ensure doors and windows remain secure



DO ensure sensitive records are locked away



DO ensure government assets remain safe and secure



DON'T



DON'T leave doors and windows open



DON'T allow unauthorised persons access into sensitive areas



DON'T leave your device unlocked when you walk away from it



POTENTIAL IMPACTS



Failed Systems



Malware



Physical Damage to Hardware

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667

HOW LONG FOR A HACKER TO BRUTE FORCE YOUR PASSWORD?



More complex passwords require extra time for hackers to brute force them. Make sure your password is not easily guessable and does not include personal details (birthday, family name, etc.).

No. of Characters	Only Numbers	UPPERCASE/ Lowercase Letters	Numbers & UPPERCASE/ Lowercase Letters	Numbers, UPPERCASE/ Lowercase Letters & Symbols
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	1 second	2 seconds	4 seconds
8	Instantly	28 seconds	2 minutes	5 minutes
9	Instantly	24 minutes	2 hours	6 hours
10	Instantly	21 hours	5 days	2 weeks
11	Instantly	1 month	10 months	3 years
12	1 second	6 years	53 years	226 years
13	5 seconds	332 years	3k years	15k years
14	52 seconds	898k years	12m years	77m years
15	9 minutes	2bn years	48bn years	380bn years

Information from <https://www.hivesystems.io/password>

For more information:



helpdesk@sig.gov.sb



(+677) 24580 / 27668 / 27667