



PROPOSED ARIN / CARIBNOG 1-DAY SEMINAR PROGRAMME

Securing Our Digital Foundations

Understanding Internet Security and Why It Matters

Proposed Date	1 or 2 October 2026
Time	9:00 a.m. – 3:00 p.m.
Format	Presentations, Interactive Sessions and Hands On Exercises
Country	St. Kitts and Nevis

About the Program

The programme is designed to move participants from understanding how Internet trust works, through the risks that can undermine it, to the practices and cooperation that strengthen security and resilience. Technical concepts would be introduced through practical examples, demonstrations and discussion rather than specialist instruction.



Securing Our Digital Foundations: *Understanding Internet Security and Why It Matters*

PROVISIONAL AGENDA

Time	Session	Purpose and Approach
9:00–9:30	Opening and Context Setting	Government welcome and seminar framing. Position the session within national digital priorities and establish its complementary relationship to the Cybersecurity Week that follows.
INTERNET FUNDAMENTALS		
9:30–10:00	Internet 101: How Does the Internet Know Where to Go?	An accessible introduction to how networks connect and Internet traffic reaches its destination. Introduce IP addresses, Internet number resources, autonomous networks and routing only to the level needed for the security discussions that follow.
10:00–10:40	Routing Security 101: Can We Trust the Route?	Explore what happens when routing information is wrong, misconfigured or maliciously manipulated. Introduce route leaks, hijacks and RPKI through practical examples and visual demonstration.
10:40–10:55	Break	
THE TRUST INFRASTRUCTURE		
10:55–11:35	DNS Security 101: Can We Trust the Destination?	Explain the role of DNS through familiar Internet experiences, the risks created when naming information cannot be trusted, and how DNSSEC strengthens confidence in the system.
11:35–12:15	When Trust Breaks	Interactive scenario session bringing routing and DNS together. Mixed participant groups consider what happened, who is affected, why it matters and what actions could prevent or mitigate the problem.
12:15–12:55	Lunch	
SECURING OUR DIGITAL FUTURE		
12:55–1:35	Resilience Close to Home	Connect Internet-wide mechanisms to the national environment: local interconnection, dependencies, visibility, redundancy, resilience and appropriate network autonomy. Use SKNIX as a practical local reference point.
1:35–2:15	Trust Communities: Securing the Internet Together	Examine why Internet security depends on cooperation, trusted relationships, information sharing, common practices and participation in technical communities across organisational and national boundaries.
2:15–2:45	From Understanding to Action: Strengthening Our Digital Foundations	Interactive translation of the day's lessons into a concise set of recommended Internet security and resilience practices. Participants use a practical checklist to consider why each practice matters, who needs to be involved and what next steps should be considered.
2:45–3:00	Closing: Securing Our Digital Foundations	Draw together the principal lessons, invite brief participant reflections — including student perspectives — and establish the handover into the activities of Cybersecurity Week.