Lab 3

Pretexts

Group 2

**, Abdul-Ramon Adeyemi Folarin, & **

**, , , & **

School of Information Technology Administration & Security, Seneca Polytechnic

DPI914NIA: Social Engineering

Professors Chris Robertson & Suranjit Paul

May 27, 2026

Student Integrity Statement: I/we declare that the attached assignment is my/our own work in accordance with the Seneca Academic Policy. No part of this assignment has been copied manually or electronically from any other source (including web sites) or distributed to other students

Table of Contents

1. Introduction....2
2. Victim Identification....2
3. Pretexts....3
Pretext #1: Microsoft Office 365 Tenant Administrator Re-Verification....3
Pretext #2: SSL Certificate Expiry Notice (Seneca Web Infrastructure)....5
Pretext #3: VMware License Renewal and Data Center Audit....7
Pretext #4: Seneca IT Security Audit - Data Center Access Re-Authorization....9
4. Conclusion....11
References....12

1. Introduction

This report demonstrates the process an attacker follows when planning a targeted social engineering campaign: identifying a high-value victim through open-source intelligence (OSINT) and developing believable pretexts for use in a spear-phishing attack.

All information gathered for this report was obtained exclusively from publicly available sources, including LinkedIn and Seneca Polytechnic's internal ITS organizational chart, which was made available online and was a good factor for reconnaissance of choosing our target. No internal systems, credentials, or non-public Seneca data were accessed. Professor Chris Robertson has confirmed that former Seneca employees are a valid target for this lab exercise.

2. Victim Identification

Target:

Role (at time of employment): / IT Manager, Data Centre Services, Seneca College ( )

Explanation: was selected as the target because his combined role history at Seneca College and his publicly available LinkedIn profile demonstrate one of the highest levels of privileged infrastructure access of any identifiable former staff member. spent approximately at Seneca ( ), holding two successive roles: IT Manager, Data Centre Services, and later . [1]

Seneca's ITS organizational chart confirms that the Data Centre Services area, which managed, covered the following systems: Data Center operations, Microsoft Office 365, Seneca's public-facing websites, software license management, SSL certificates, physical and virtual servers, and storage infrastructure. [2] These are among the most sensitive systems at any institution. An attacker who compromised the credentials of the manager overseeing these systems would have had the ability to access and modify the college's core IT environment, including cloud tenants, web infrastructure, and server configurations across all campuses.

Compared to other identifiable Seneca ITS staff, is a stronger candidate than a front-line technician because his managerial role gave him access to administrative controls across the entire infrastructure stack, not just a subset of devices or systems. Whereas other Seneca Polytechnic employees were limited to what they were able to access based on their role/department. Chris Robertson has confirmed that past employees are valid targets for this lab, as their former credentials and access patterns remain relevant for understanding spear-phishing scenarios. [3]

His Seneca email address, following the institution's publicly documented format, would have been (prior to the 2023 rebrand to Seneca Polytechnic). [4]

3. Pretexts

Pretext #1: Microsoft Office 365 Tenant Administrator Re-Verification

Email:

From:	Microsoft 365 Admin Center < >
To:	
Subject:	Action Required: Global Administrator Account Verification - Seneca College Tenant

Microsoft 365

Dear ,

A routine security review of your organization's Microsoft 365 tenant (Tenant ID: SEN-CA-001483) has flagged your Global Administrator account for re-verification. This review is part of Microsoft's Secure Future Initiative, rolled out to all Canadian Education tenants in Q2 2022.

Your account currently holds the following administrative roles:

- Global Administrator
- Exchange Administrator
- SharePoint Administrator

To maintain uninterrupted administrative access to your organization's tenant, you must complete re-verification within 48 hours. Failure to do so will result in a temporary downgrade to standard user permissions pending a manual review by Microsoft's Enterprise Trust team.

>> Verify Your Administrator Account Now <<

[LINK PLACEHOLDER: http:// /auth/tenant]

If this request was triggered in error, contact Microsoft Enterprise Support at 1-800-865-9408, reference case #CA-2022-ETR-00482.

Regards,

Microsoft 365 Enterprise Trust Team

Microsoft Corporation | One Microsoft Way, Redmond, WA 98052

Microsoft 365 | Privacy Statement | Terms of Use | Support

Explanation:

The ITS organizational chart explicitly lists Office 365 as falling under the Data Centre Services area that [redacted] managed at Seneca. [2] As the manager of that team, he would have held Global Administrator or equivalent privileges on Seneca's Microsoft 365 tenant, making an O365 admin verification request the most direct and targeted pretext possible. The email references real Microsoft administrative role names, a plausible initiative name (Microsoft's Secure Future Initiative is a real 2023 Microsoft program, which adds credibility when used in a 2022 scenario), and a fabricated but realistic support case number. The 48-hour deadline and threat of privilege downgrade create urgency without appearing overtly aggressive. The specific role list mirrors what a real admin notification would include, which makes it feel less like a generic phishing email.

Pretext #2: SSL Certificate Expiry Notice (Seneca Web Infrastructure)

Email:

From:	DigiCert Certificate Services < >
To:	
Subject:	Urgent: SSL/TLS Certificate Expiry in 14 Days - senecacollege.ca (Order #DC-7821-CA)

digicert®

Dear ,

This is an automated renewal notice for the following SSL/TLS certificate registered under your DigiCert account (Account ID: ORG-SENECA-7821):

Domain: senecacollege.ca (and 12 SANs)

Certificate: Multi-Domain OV SSL

Expiry Date: [Date + 14 days]

Order #: DC-7821-CA

If this certificate expires without renewal, HTTPS connections to senecacollege.ca and all associated subdomains will display a browser security warning to all visitors, including students and staff. This may also trigger service interruptions for applications dependent on this certificate.

To renew your certificate and download the updated files, please log in to your DigiCert account using the link below:

>> Renew Certificate - DigiCert Account Portal <<

[LINK PLACEHOLDER: http:// /login]

If you have questions, contact your DigiCert account manager:

| |

Regards,

DigiCert Certificate Renewal Team

digicert® | digicert.com | support@digicert.com

Explanation:

SSL certificate management for Seneca's websites falls directly under the Data Centre Services area that [redacted] managed, as explicitly listed in the ITS org chart. [2] Certificate expiry is a routine but high-urgency IT event; a certificate lapse on senecacollege.ca would immediately cause browser security warnings for all students and staff, which is a very public and embarrassing failure for the manager responsible. This creates strong psychological pressure to renew immediately without additional scrutiny. DigiCert is one of the most widely used certificate authorities in Canada and is a recognizable brand to any infrastructure manager, adding legitimacy. The inclusion of a specific account manager name, extension, and a realistic order number format make the email appear to originate from a real account relationship rather than a mass phishing campaign.

Pretext #3: VMware License Renewal and Data Center Audit

Email:

From:	Broadcom / VMware Enterprise Licensing <vmware-licensing@broadcom- >
To:	
Subject:	License Renewal Required: VMware vSphere and vCenter Server - Seneca College (Contract: VMW-EDU-CA-3847)

vmware® by Broadcom

Dear ,

Your organization's VMware vSphere and vCenter Server licenses are approaching their renewal date under the VMware Education Institution Agreement (Contract: VMW-EDU-CA-3847).

Product: VMware vSphere Enterprise Plus (25 CPU licenses)

Product: VMware vCenter Server Standard

Expiry Date: [Date + 30 days]

Contract Ref: VMW-EDU-CA-3847

As the registered technical administrator for Seneca College's VMware environment, your action is required to initiate the renewal and apply updated license keys to your vCenter deployment.

Unrenewed licenses will enter a 30-day grace period, after which vSphere hosts will revert to Essentials-tier feature limits, affecting virtual machine management across your data center.

>> Log In to VMware Customer Connect and Renew Licenses <<

[LINK PLACEHOLDER: http:// /login]

For assistance, contact your VMware account representative:

| |

Regards,

VMware by Broadcom - Enterprise Licensing

vmware by Broadcom | vmware.com | customerconnect@vmware.com

Explanation:

's role explicitly covered servers and storage at Seneca's data center. [2] VMware vSphere is the industry-standard virtualization platform used in enterprise data centers, and its management through vCenter Server is a core tool for any infrastructure manager overseeing a multi-server environment. A license expiry notice referencing vSphere and vCenter is therefore exactly the type of email would expect to receive as part of his regular administrative responsibilities. The threat of vSphere feature degradation affecting virtual machine management provides a realistic and proportionate consequence that an infrastructure manager would want to prevent. The timing of this pretext aligns with VMware's 2023 acquisition by Broadcom, which triggered widespread real license renewal and migration communications across the industry, making spoofed Broadcom/VMware emails particularly difficult to distinguish from genuine ones during that period.

Pretext #4: Seneca IT Security Audit - Data Center Access Re-Authorization

Email:

From:	Seneca College ITS Security and Compliance < itservicedesk@senecapolytechnic.ca >
To:	
Subject:	Mandatory: Annual Data Centre Access Re-Authorization - Deadline: [Date + 10 days]

Seneca POLYTECHNIC

Dear ,

As part of Seneca College's annual IT Governance and Access Control Review (ITS-GOV-2022-09), all staff with administrative access to Seneca's Data Centre environment are required to complete a mandatory re-authorization of their access privileges.

Your account has been identified as holding the following administrative access levels:

- Physical Data Centre access (Newnham and Markham locations)
- vCenter Server administrative rights
- Microsoft 365 tenant administration
- Storage Area Network (SAN) management credentials

To maintain uninterrupted access and remain compliant with ITS Policy ITS-POL-2022-14, please complete your re-authorization through the ITS Governance Portal before [Date + 10 days]. Accounts not re-authorized by this deadline will be placed under a temporary access review pending manual verification by the Security and Compliance Office.

>> Complete Data Centre Access Re-Authorization <<

[LINK PLACEHOLDER: http:// /reauth/datacenter]

For questions, contact the ITS Security and Compliance Office:

Joseph Lee | Manager, Security and Compliance | ext. 55190

Regards,

ITS Security and Compliance Office

Information Technology Services | Seneca College
Seneca POLYTECHNIC | senecacollege.ca | itservicedesk@senecapolytechnic.ca.

Explanation:

This pretext is particularly strong because it uses real names and real organizational details sourced directly from Seneca's ITS org chart. The Security and Compliance Office is a real ITS department, and Joseph Lee is the real manager of that office, both confirmed by the published org chart. [2] Referencing a real colleague by name adds a layer of social proof that would make [redacted] significantly less likely to question the email's authenticity. The access levels listed in the email (physical data center access, vCenter rights, O365 tenant administration, SAN management) are directly derived from the scope of his publicly documented role, making the list feel targeted and accurate rather than generic. Impersonating an internal compliance request is effective because it leverages authority from within the same organization, and the threat of access suspension on systems the target actively manages provides strong motivation to act without scrutinizing the sender address. [1] [2]

4. Conclusion

This lab demonstrates how a small amount of publicly available information can be sufficient to identify a high-value target and construct multiple convincing spear-phishing pretexts. [redacted]'s LinkedIn profile and Seneca's published ITS organizational chart together provided his name, role, the specific systems he administered, his certifications, his career timeline, and the names of his internal colleagues. All of this information was obtained without accessing any internal Seneca systems or restricted data.

The four pretexts developed in this report each target a different attack surface tied directly to his documented responsibilities: Microsoft 365 tenant administration, SSL certificate management, VMware data center licensing, and internal IT compliance. In every case, the believability of the pretext is a direct product of the OSINT gathered beforehand. This exercise highlights that detailed professional profiles and published organizational charts represent a meaningful attack surface for social engineering, and that limiting publicly available technical detail is a practical risk mitigation measure for IT organizations.

References

[1] A. [redacted], "[redacted] LinkedIn profile," LinkedIn. [Online]. Available: [redacted]. [Accessed: May 21, 2026].

[2] Seneca Polytechnic, "ITS Organizational Chart.jpg," Seneca Polytechnic Student Hub, Information Technology Services. [Online]. Available: https://students.senecapolytechnic.ca/spaces/187/it-strategies-and-policies/files/1241/its-organizational-chart-jpg. [Accessed: May 21, 2026].

[3] C. Robertson, "DPI914 Social Engineering class discussion," Seneca Polytechnic, Zoom class discussion, May 21, 2026. Personal communication.

[4] Seneca Polytechnic, "Information Technology Services (ITS)," Seneca Polytechnic Student Hub. [Online]. Available: https://students.senecapolytechnic.ca/spaces/114/information-technology-services/home. [Accessed: May 21, 2026].

[5] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed. Indianapolis, IN, USA: Wiley, 2018.

[6] S. Conheady, Social Engineering in IT Security: Tools, Tactics and Techniques. New York, NY, USA: McGraw-Hill Education, 2014.