Network Security Advice

1. Router Security Check:

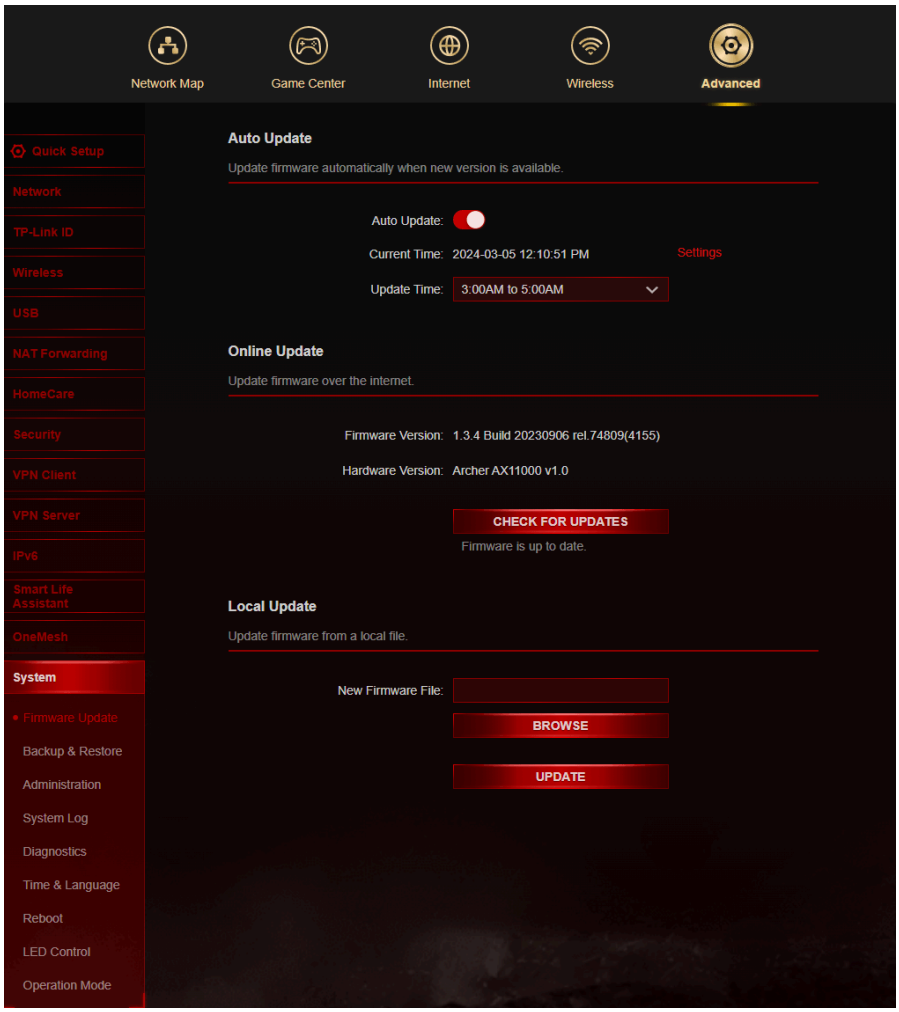
Router Model and Details:

- Firmware Version: 1.3.4 Build 20230906 rel.74809(4155)
- Hardware Version: Archer AX11000 v1.0

Instructions for Firmware Update:

- Check for firmware updates regularly to patch security vulnerabilities.
- Steps to update firmware:
    1. Log in to the router's web interface.
    2. Navigate to the "System Tools" or "Management" section.
    3. Look for the "Firmware Upgrade" or "System Update" option.
    4. Download and install the latest firmware version.
    5. Verify successful updates and restart the router if required.

Screenshot of Router Firmware Update Option



2. Setting up Guest Network:

Router Login Details:

- Username: [Your Router Admin Username]
- Password: [Your Router Admin Password]

Guest Network Setup Details:

- Benefits of having a guest network:
    - Isolates guest devices from the main network.
    - Prevents unauthorized access to sensitive data.
- Steps to enable and configure the guest network:
    1. Log in to the router's web interface.
    2. Navigate to the "Guest Network" or "Wireless" section.
    3. Enable the guest network feature.
    4. Set a unique SSID (network name) and password for the guest network.
    5. Configure security options (e.g., WPA2-PSK encryption).

Security Considerations:

- Advise guests to use the guest network for internet access.
- Regularly change the guest network password for added security.

3. Educating About Phishing:

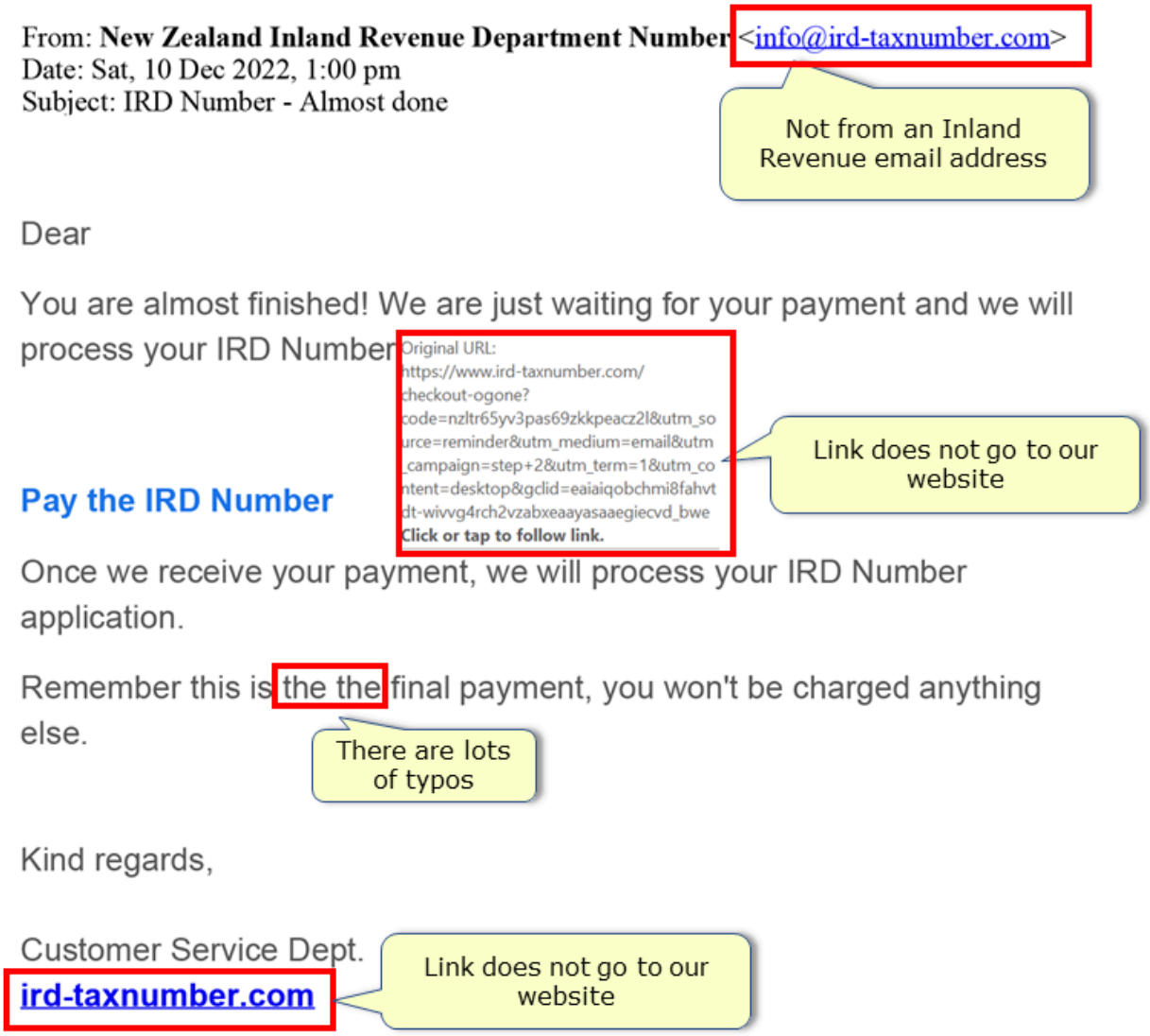
Guide on Phishing:

- Overview of phishing attacks and their impact on cybersecurity.
- Explanation of common phishing tactics:
    - Email spoofing, deceptive links, urgent requests for personal information.
- Phishing Examples:
    1. "Your Account Has Been Compromised" Email
    2. "Click Here to Claim Your Prize" Scam

Recognizing Phishing Emails:

- Characteristics of phishing emails:
    - Poor grammar, spelling errors, unexpected sender addresses.
- What to Do When You Receive a Suspicious Email:
    1. Do not click on links or download attachments.
    2. Report the email as phishing or suspicious.

Example of Phishing Email from Inland Revenue



4. Password Management:

Password Guidelines:

- Create strong passwords using a mix of letters, numbers, and symbols.
- Avoid using easily guessable information (e.g., birthdays, names).
- Example of a strong password: "P@ssw0rd123!#"

Regular Password Changes:

- Set a schedule for changing passwords (e.g., every 3 months).
- Use different passwords for each account to prevent credential stuffing attacks.

Introduction to Password Managers:

- Benefits of using password managers:
    - Securely store and manage passwords.
    - Generate strong, unique passwords for each account.
- Recommended Password Managers:
    1. LastPass

        - Description: LastPass is a popular password manager known for its user-friendly interface and robust security features. It securely stores all your passwords in an encrypted vault, accessible with a single master password.
        - Key Features:
            - Secure password generation.
            - Autofill login credentials on websites.
            - Two-factor authentication for added security.
            - Secure password sharing with trusted contacts.
    2. Dashlane

        - Description: Dashlane is a comprehensive password manager with a focus on simplicity and strong encryption. It offers a seamless way to manage passwords across devices while prioritizing user privacy.
        - Key Features:
            - Secure password storage and syncing across devices.
            - Automatic password changer for supported websites.
            - Secure note storage for sensitive information.
            - Dark web monitoring to alert you of potential data breaches.
    3. Bitwarden

        - Description: Bitwarden is an open-source password manager known for its transparency and flexibility. It provides strong encryption for your passwords and offers convenient features for secure password management.
        - Key Features:
            - Open-source and audited for security.
            - Cross-platform support (Windows, Mac, Linux, iOS, Android).
            - Secure password sharing and organization.
            - Self-hosting option for advanced users.