Analyze a Phishing Email Sample

Date: June 24, 2025

1 Sample Phishing Emails Overview

This report analyzes three hypothetical phishing emails based on common attack patterns.

1.1 Email 1: PayPal Account Suspension

Subject: URGENT: Your Account Has Been Suspended – Verify Now!

Sender: PayPal Security <service@paypal-secure.net>

Recipient: user@example.com

Body Summary: Claims account suspension, urges verification via a link, includes PDF attachment "Account_Security_Details.pdf."

Header Excerpt:

```
Received: from unknown (HELO mail.paypal-secure.net) (192
Authentication-Results: spf=fail (sender IP is 192.168.0.1)
From: PayPal Security <service@paypal-secure.net>
```

1.2 Email 2: Bank Password Reset

Subject: Immediate Action Required: Reset Your Password

Sender: Wells Fargo Alerts <alert@wellsfargo-support.com>

Recipient: customer@example.com

Body Summary: Alleges unauthorized login, prompts password reset via link, contains typo "immedaitely."

Header Excerpt:

```
Received: from [10.0.0.5] (HELO mail.wellsfargo-support.c
Authentication-Results: spf=none; dkim=fail
From: Wells Fargo Alerts <alert@wellsfargo-support.com>
```

1.3 Email 3: Invoice Payment Due

Subject: Overdue Invoice INV-4532 – Pay Now to Avoid Penalties

Sender: Accounts Dept <billing@quickbooks-online.org>

Recipient: business@example.com

Body Summary: Claims overdue invoice, demands payment via link, includes Excel attachment "Invoice_4532.xls."

Header Excerpt:

```
Received: from unknown (HELO smtp.quickbooks-online.org)
Authentication-Results: spf=fail
From: Accounts Dept <billing@quickbooks-online.org>
```

2 Analysis Process

Emails were examined for sender domains, headers, links, attachments, language, URLs, and errors.

2.1 Sender Email Address

- **Email 1**: `paypal-secure.net` mimics "paypal.com."
- **Email 2**: `wellsfargo-support.com` differs from "wellsfargo.com."
- **Email 3**: `quickbooks-online.org` not "quickbooks.intuit.com."
- **Phishing Indicator**: Spoofed sender domains.

2.2 Email Header Analysis

- **Tool**: MxToolbox or Googles Message Header Analyzer.
- **Findings**:
  - **Email 1**: Private IP (192.168.0.1), SPF fail.
  - **Email 2**: Internal IP (10.0.0.5), SPF none, DKIM fail.
  - **Email 3**: Private IP (172.16.1.2), SPF fail.
- **Phishing Indicator**: Authentication failures, suspicious IPs.

2.3 Suspicious Links and Attachments

- **Email 1**: Link `http://paypal-secure.net/verify`, PDF attachment.
- **Email 2**: Link `https://wellsfargo-support.com/reset`.
- **Email 3**: Link `https://quickbooks-online.org/pay`, XLS attachment.
- **Phishing Indicator**: Non-official URLs, risky attachments.

2.4 Urgent or Threatening Language

- **Email 1**: "Suspend"; "24 hours."
- **Email 2**: "Unauthorized login"; "immediately."
- **Email 3**: "Overdue"; "48 hours."
- **Phishing Indicator**: Fear-inducing language.

2.5 Mismatched URLs

- **Email 1**: "Verify Now" to `http://paypal-secure.net/verify`.
- **Email 2**: "Reset Password" to `https://wellsfargo-support.com/reset`.

- **Email 3**: “Pay Now” to https://quickbooks-online.org/pay.
- **Phishing Indicator**: URL mismatches.

2.6 Spelling and Grammar Errors

- **Email 1**: “Verfiy” for “verify.”
- **Email 2**: “Immedaitely” for “immediately.”
- **Email 3**: Generic phrasing.
- **Phishing Indicator**: Typos, generic language.

3 Phishing Traits Summary

- Spoofed domains (e.g., paypal-secure.net).
- Header failures (e.g., SPF fail, private IPs).
- Malicious URLs (e.g., https://wellsfargo-support.com/reset).
- Risky attachments (PDF, XLS).
- Urgent language (e.g., “24 hours” hours).
- Typos (e.g., “verfiy”verfy).

4 Recommendations

- Avoid links, attachments.
- Sandbox attachments (e.g., VirusTotal).
- Report phishing.
- Verify via official sites (https://paypal.com, https://wellsfargo.com,
- https://quickbooks.intuit.com).
- Educate users.

5 Tools

- Email client (e.g., Gmail).
- Header analyzer (e.g., MxToolbox).

6 Conclusion

The emails are phishing attempts, using spoofing, malicious links, and typos. Recognizing these prevents attacks.