Phishing Awareness Guide

Document ID: IT-SEC-012 **Last Updated:** 2024-02-15 **Owner:** Security Team **Classification:** Internal

---

What is Phishing?

Phishing is a social engineering attack where attackers attempt to trick you into revealing sensitive information, clicking malicious links, or downloading malware by impersonating trusted entities.

Types of Phishing

Email Phishing

Mass emails that appear to come from legitimate sources.

Example: > Subject: Urgent: Your account will be suspended > > Dear Customer, > Your NovaTech account will be suspended in 24 hours unless you verify your information immediately. > Click here to verify: [malicious-link.com]

Spear Phishing

Targeted attacks using personalized information.

Example: > Subject: Re: Q3 Budget Review > > Hi Sarah, > Following up on our conversation with Michael yesterday. Can you review the attached budget spreadsheet? > [malicious-attachment.xlsx]

Whaling

Phishing targeting executives and senior leaders.

Example: > From: ceo@novatech-support.com (not real domain) > Subject: Urgent wire transfer needed > > I need you to process an urgent wire transfer for a confidential acquisition. Please keep this between us.

Smishing (SMS Phishing)

Phishing via text messages.

Example: > NovaTech IT: Your password expires today. Reset immediately at: bit.ly/suspicious-link

Vishing (Voice Phishing)

Phishing via phone calls.

Example: > "This is IT support. We detected unusual activity on your account. I need to verify your password to secure your account."

Red Flags

Sender Red Flags

Suspicious email address - Display name doesn't match email - Misspelled domain (novateck.com vs novatech.com) - Free email domains for "official" messages

External sender warning - Email claims to be internal but shows external warning - "CEO" sending from gmail.com

Content Red Flags

Urgency and threats - "Act immediately or your account will be closed" - "You have 24 hours to respond" - Threatening language

Too good to be true - You've won something - Unexpected refund or bonus - Free gift cards

Unusual requests - Asking for passwords or credentials - Requesting wire transfers - Asking to bypass normal procedures

Poor grammar and spelling - Multiple typos - Awkward phrasing - Inconsistent formatting

Link Red Flags

Suspicious URLs - Hover to preview (don't click) - Misspelled domains - HTTP instead of HTTPS - Unusual URL structures

Shortened URLs - bit.ly, tinyurl, etc. hide real destination - Especially suspicious in business context

Attachment Red Flags

Unexpected attachments - Files you didn't request - Unusual file types (.exe, .scr, .zip) - "Enable macros" or "enable content" prompts

---

Real Examples at NovaTech

Example 1: Fake IT Support

The Attack: > From: it-helpdesk@novatech-support.net > Subject: Password Expiration Notice > > Your network password will expire in 2 hours. Click below to reset: > [fake-novatech-login.com]

Red Flags: - Wrong domain (novatech-support.net vs novatech.com) - External email claiming to be IT - Urgency (2 hours) - We don't send password reset links this way

Example 2: Executive Impersonation

The Attack: > From: Sarah Chen sarah.chen.ceo@gmail.com > Subject: Quick favor > > Are you available? I need you to purchase some gift cards for a client appreciation. I'll reimburse you. Keep this confidential.

Red Flags: - Gmail address, not company email - Unusual request (gift cards) - Request for confidentiality - "Quick favor" tactic

Example 3: Invoice Fraud

The Attack: > From: accounts@vendor-name.com > Subject: Updated Payment Information > > Please note our bank details have changed. All future payments should go to the following account: [fraudulent account]

Red Flags: - Unsolicited banking change - No prior communication - Verify through known contact

---

What to Do

If You Receive a Suspicious Email

1. **Don't click** any links or attachments

2. **Don't reply** to the sender
3. **Report it:**
    - Click "Report Phishing" button in Gmail
    - Forward to security@novatech.com
    - Post in #security-questions if unsure
4. **Delete** the email after reporting

If You Clicked a Link

1. **Stop** - don't enter any information
2. **Disconnect** from network if malware suspected
3. **Report immediately** to #security-urgent
4. **Change passwords** if you entered credentials
5. **Run scan** via Self Service app

If You Entered Credentials

1. **Change password immediately** (from a different device)
2. **Report to Security** - #security-urgent
3. **Check account activity** for unauthorized access
4. **Enable/verify MFA** is active

If You Opened an Attachment

1. **Disconnect from network** (WiFi off, unplug ethernet)
2. **Don't turn off computer** (preserves evidence)
3. **Report immediately** to #security-urgent
4. **Wait for Security team** to investigate

Prevention

Technical Protections

NovaTech has implemented: - Email filtering and scanning - Link protection and rewriting - Attachment sandboxing - External email warnings - Phishing simulations

Personal Protections

Verify before acting: - Call the sender using known number - Check with IT for unusual IT requests - Verify wire transfers through normal process

Practice good habits: - Use unique passwords (1Password) - Enable MFA everywhere - Keep software updated - Lock your computer

Stay informed: - Complete security training - Read security bulletins - Attend awareness sessions

---

Phishing Simulations

What They Are

NovaTech conducts periodic phishing simulations to: - Test our defenses - Train employees to recognize phishing - Identify areas for improvement

If You Click a Simulation

- You'll see a training page
- Complete the brief training
- No disciplinary action for simulation clicks
- Use it as a learning opportunity

Tracking and Reporting

- Anonymous aggregate data
- Used to improve training
- Focus on education, not punishment

Resources

Report Phishing

- Gmail: "Report Phishing" button
- Email: security@novatech.com
- Slack: #security-urgent (if urgent)

Get Help

- Slack: #security-questions
- IT Help: #it-help

Learn More

- Security training: [Learning Portal]
- Security wiki: [Internal Link]
- Monthly security newsletter

Quick Reference Card

When in doubt, check it out!

Red Flag	Action
Urgent request	Slow down, verify
Request for credentials	Never share via email
Unexpected attachment	Don't open, report
Suspicious link	Hover don't click, report
Financial request	Verify via phone
"From" CEO/exec	Check email address carefully

Report to: security@novatech.com or "Report Phishing" button

Related Documents: Security Best Practices (IT-SEC-010), Incident Response Plan (IT-SEC-020), Acceptable Use Policy (IT-SEC-015)