Phishing Reporting Process

Document Number: IT-SEC-005 **Effective Date:** January 1, 2020 **Last Updated:** October 1, 2023 **Owner:** IT Security **Applies To:** All employees globally

Overview

Phishing attacks are one of the most common threats to NovaTech. This document explains how to identify, report, and respond to phishing attempts.

What is Phishing?

Phishing is an attempt to steal information or compromise systems by impersonating a legitimate person, company, or service. Common types include:

Email Phishing

- Fake emails appearing to be from trusted sources
- Requests to click links or download attachments
- Often creates urgency ("Immediate action required!")

Spear Phishing

- Targeted attacks using personal information
- May reference real projects, colleagues, or events
- More sophisticated and believable

Business Email Compromise (BEC)

- Impersonating executives or colleagues
- Requests for wire transfers, gift cards, or sensitive data
- Often uses similar email addresses

Smishing (SMS Phishing)

- Phishing via text message
- Links to malicious websites
- Fake urgent notifications

Vishing (Voice Phishing)

- Phone calls impersonating legitimate organizations
- Requests for passwords or verification codes
- Social engineering tactics

How to Identify Phishing

Red Flags

Warning Sign	Example
Urgency/pressure	"Act immediately or your account will be suspended"
Suspicious sender	email@novattech.com (extra 't') vs @novatech.com
Generic greeting	"Dear Customer" instead of your name
Spelling/grammar errors	Professional organizations rarely have errors
Unusual requests	CEO asking you to buy gift cards
Mismatched URLs	Link text says one thing, actual URL is different
Unexpected attachments	Invoice from unknown sender
Requests for credentials	"Verify your password"

Checking Suspicious Emails

Check the sender: 1. Click on sender name to reveal full email address 2. Verify domain is exactly correct (novatech.com, not n0vatech.com) 3. Check if you expected communication from this person

Check links (without clicking): 1. Hover over links to preview URL 2. Look for misspelled domains 3. Be suspicious of URL shorteners in professional emails

Verify through another channel: 1. If supposedly from a colleague, message them on Slack 2. If from a vendor, call their known phone number 3. Never use contact info provided in the suspicious email

Reporting Phishing

Method 1: Forward to Security (Recommended)

Forward suspicious emails to: **phishing@novatech.com**

Include: - Original email as attachment (preferred) or forwarded - Brief description of why it's suspicious - Whether you clicked any links or downloaded attachments

Method 2: Report via Outlook/Gmail

Gmail: 1. Open the email 2. Click the three dots menu 3. Select "Report phishing"

Outlook: 1. Open the email 2. Click "Report" button in toolbar 3. Select "Phishing"

Method 3: Slack

For urgent situations or questions: - Post in #security-alerts - DM any member of the Security team - Include screenshot if possible

What Happens After You Report

Security Team Response

1. **Acknowledgment** - You'll receive confirmation within 2 hours
2. **Analysis** - Security team investigates the report
3. **Action** - If malicious:
    - Email blocked across organization
    - Sender domain blocked if warranted
    - Alert sent if widespread campaign
4. **Feedback** - You may receive follow-up on confirmed threats

No Punishment for Reporting

- **You will never be punished for reporting suspicious emails**
- False positives are expected and appreciated
- Better to report 10 legitimate emails than miss 1 phishing attempt

If You Clicked or Responded

Immediate Actions

If you clicked a link: 1. Disconnect from VPN (but stay connected to internet) 2. Report to phishing@novatech.com immediately 3. Note what you saw/did after clicking 4. Run CrowdStrike scan (it may prompt automatically) 5. Await further instructions from Security

If you entered credentials: 1. Change that password IMMEDIATELY (use another device if possible) 2. Report to phishing@novatech.com 3. Enable MFA if not already enabled 4. Check for unauthorized access to that account 5. Security may require additional password changes

If you downloaded/opened an attachment: 1. Disconnect from VPN 2. Do not restart your computer 3. Report immediately to phishing@novatech.com 4. Security team will provide further instructions 5. Device may need forensic analysis

If you sent money or gift cards: 1. Contact Finance immediately (finance-ops@novatech.com) 2. Report to Security 3. Contact your bank if personal accounts affected 4. Document everything

Don't Panic

- Mistakes happen - the important thing is to report quickly
- Early reporting minimizes damage
- There's no punishment for falling victim if you report promptly

Phishing Simulations

What They Are

IT Security conducts periodic phishing simulations: - Test organizational awareness - Identify training needs - Measure improvement over time

How They Work

- Look like real phishing attempts
- Safe to click (tracked, not malicious)
- May lead to training if "failed"
- Part of security awareness program

Not Punitive

Simulations are educational: - No disciplinary action for clicking - Training provided to those who need it - Anonymous aggregate reporting

Prevention Tips

Email Safety

- Verify unexpected requests through another channel
- Don't click links in emails - navigate to sites directly
- Be suspicious of urgency and pressure tactics
- When in doubt, report it

Account Security

- Use strong, unique passwords
- Enable MFA everywhere
- Use 1Password for credential management
- Never share passwords or MFA codes

General Awareness

- Attackers may research you on LinkedIn
- Verify identity through known channels
- Trust your instincts - if something feels wrong, investigate

Recent Phishing Trends

Security regularly updates the organization on active threats: - Check #security-alerts for current campaigns - Monthly security newsletter includes recent examples - Training updated based on real attempts

Training

Required Training

All employees complete annual security awareness training: - Includes phishing identification module - Interactive examples - Assigned in Workday Learning

Additional Resources

- Security Office Hours (weekly, see calendar)
- #security-questions Slack channel
- Security Awareness Training (IT-SEC-001)

FAQ

Q: Is it okay to forward the suspicious email? A: Yes! Forward to phishing@novatech.com. For best analysis, forward as attachment.

Q: What if the email is actually legitimate? A: No problem! We'd rather investigate false positives than miss real threats.

Q: Can I delete suspicious emails instead of reporting? A: Please report first. This helps protect others who may receive the same email.

Q: What if I'm not sure if it's phishing? A: Report it. Our team will analyze and let you know.

Q: How do I report smishing (text message phishing)? A: Screenshot and email to phishing@novatech.com with description.

Emergency Contacts

For urgent security issues: - **Email:** phishing@novatech.com - **Slack:** #security-alerts - **Phone:** 1-800-555-0196 (24/7) - **After hours:** security-oncall@novatech.com

---

Related Documents: Security Awareness Training (IT-SEC-001), Incident Response Procedures (IT-SEC-010), Password Requirements (IT-ACC-006)