Novatech

www.novatech-global.com

Phishing Prevention Tips

Recognize Phishing Attempts

- **Urgent Requests:** Be cautious of emails demanding immediate action, such as threats to close your account or impose penalties.
- **Suspicious Senders:** Check email addresses for typos or inconsistencies (e.g., "amaz0n.com" instead of "amazon.com").
- **Unfamiliar Links:** Hover over links before clicking to verify the actual URL. Avoid clicking on links in unsolicited emails.
- **Grammar and Spelling Errors:** Phishing emails often contain mistakes that can be a giveaway.
- **Requests for Sensitive Information:** Never provide passwords, credit card details, or social security numbers in response to unsolicited emails.

Novatech

www.novatech-global.com

Educate and Train Employees

2

- **Cybersecurity Awareness Training:** Educate staff to recognize phishing tactics and report suspicious emails promptly.
- **Phishing Simulations:** Conduct regular tests to evaluate employees' ability to spot fake emails and improve their vigilance.
- **Password Policies:** Enforce strong, unique passwords and the use of password managers

Use Technical Protections

3

- **Anti-Phishing Software:** Deploy solutions that scan emails and block malicious links or attachments in real time.
- **AI-Powered Email Security:** Implement AI tools to detect sophisticated phishing attempts, including those using generative AI.
- **Multi-Factor Authentication (MFA):** Add an extra layer of security by requiring a second form of verification for sensitive accounts.
- **Browser Security Extensions:** Use extensions that identify and block phishing sites through AI and image recognition.

Foster a Reporting Culture

4

- **Empower Employees:** Encourage staff to report suspicious emails, links, or calls through multiple channels.
- **Open Communication:** Create a safe environment where employees can collaborate with security teams without fear of punishment.
- **Reward Reporting:** Acknowledge and reward employees who report phishing attempts to reinforce proactive security practices

Novatech

www.novatech-global.com

Update and Patch Systems

5

- **Regular Updates:** Keep software and operating systems up to date to close vulnerabilities targeted by phishing attacks.
- **Vulnerability Scans:** Conduct routine scans to identify and address weaknesses in your systems.

Novatech

www.novatech-global.com

Develop Clear Policies

6

- **Data Security Policies: O**utline acceptable use of company resources, data handling procedures, and protocols for reporting phishing attempts.
- **Enforcement:** Regularly audit policies and enforce compliance to maintain a secure organizational culture.

Novatech

www.novatech-global.com

Report Phishing Attempts

7

- **Notify Authorities:** Report phishing attacks to organizations like the FTC, ISPs, and anti-phishing groups (e.g., APWG).
- **Forward Suspicious Emails:** Send phishing emails as attachments to your IT department or CISA.

Novatech

www.novatech-global.com

KEY TAKEAWAYS

- Phishing relies on deception, so vigilance and training are critical.
- Technical safeguards like AI and MFA can significantly reduce risks.
- A culture of reporting and proactive updates ensures long-term protection.

Novatech

www.novatech-global.com