# PHISHING
## TOP 10 BEST PRACTICES

With the advent of AI, phishing emails have the potential to sound more legitimate and closer to the truth. Employing the practices listed below will help us defend ourselves against these attacks.

| | | Effort | Cost |
|---|---|---|---|
| 1 | **Training & Awareness:** It is important for employees to undergo training that provides understanding of phishing and equips them with the ability to recognize when they are being targeted and how to respond effectively. To enhance awareness, training against phishing must be a compulsory part of the onboarding process for new hires. It is also recommended that employees undergo these training sessions annually and when they fail a mock phishing exercise. | ★★★☆ | ★☆☆☆ |
| 2 | **Mock phishing exercise:** This helps employees get a look and feel for what this attack is like in the real-world. These exercises also allow organizations to assess their employees' susceptibility to these attacks and identify areas where additional training may be needed. | ★★☆☆ | ★★☆☆ |
| 3 | **Spam filters:** Implement spam filters to prevent unwanted emails from reaching employee inboxes. | ★☆☆☆ | ★☆☆☆ |
| 4 | **Exercise caution against unsolicited emails:** Maintain a healthy level of skepticism towards emails that you did not expect to receive. Never trust, and always verify the source of unsolicited emails. This also applies to emails from co-workers that are unexpected and appear abnormal. | ★★☆☆ | ☆☆☆☆ |
| 5 | **Verify links:** Hover over links in emails to check their actual destination before clicking. | ★☆☆☆ | ☆☆☆☆ |
| 6 | **Reporting:** Encourage employees to report any suspected phishing attempts to the IT department. This can help prevent future attacks. | ★☆☆☆ | ☆☆☆☆ |
| 7 | **Multifactor Authentication (MFA):** Implementing MFA adds an extra layer of security, making it harder for attackers to gain access to accounts. | ★★☆☆ | ★★☆☆ |
| 8 | **Antivirus software:** Install and update antivirus software to protect against malware that may be delivered via phishing attacks. | ★★★☆ | ★★★☆ |
| 9 | **Firewalls:** Use firewalls to block unauthorized access to your network. | ★★★★ | ★★★★ |
| 10 | **Maintaining regular backups:** Having backups ensures that even if the phishing attack results in data loss, corruption, or ransomware encryption, the organization can restore the affected data from the backups, thereby minimizing the impact of the attack. | ★★★★ | ★★★☆ |

Using two-factor authentication, antivirus solution, maintaining up-to-date software, and implementing firewalls are effective measures that can provide a safety net if a phishing email link is inadvertently clicked.


**References:**
Microsoft Security Copilot
Top Five Best Practices For Preventing Phishing Attacks (forbes.com)
Top 10 Anti-Phishing Best Practices (infosecinstitute.com)
The 10 best practices for identifying and mitigating phishing (infosecinstitute.com)


CYBER ALBERTA