**Problem-solution fit:**

Cyber criminals use phishing emails because it's easy, cheap and effective. Email addresses are easy to obtain, and emails are virtually free to send. With little effort and cost, attackers can quickly gain access to valuable data.

The data that cybercriminals go after includes personal identifiable information (PII)—like financial account data, credit card numbers and tax and medical records—as well as sensitive business data, such as customer names and contact information, proprietary product secrets and confidential communications.

Cybercriminals also use phishing attacks to gain direct access to email, social media and other accounts or to obtain permissions to modify and compromise connected systems, like point-of-sale terminals and order processing systems. Many of the biggest data breaches, like the headline-grabbing 2013 Target breach, start with a phishing email. By using a seemingly innocent email, cybercriminals can gain a small foothold and build on it.

Solution:

Using anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer. Anti-malware is included to prevent other types of threats. Similar to anti-spam software, anti-malware software is programmed by security researchers to spot even the stealthiest malware.

Architecture:

