IronVest

IronVest Report

7 Most Dangerous Phishing Attacks

IronVest

2022 Phishing Attacks Report

Most Common and Dangerous Phishing Attack of the Year

Top 7 most common and most dangerous phishing attacks.

Note: these examples have been simplified to demonstrate the concept, but in reality can be complex and sophisticated.

1. Impersonating a well-known organization's domain
2. Impersonating a well-known organization's name
3. Impersonating your own domain
4. Impersonating your own organization's name
5. Impersonating an employee (including a CEO)
6. Hijacked domain
7. Impossible-for-human-to-detect attack

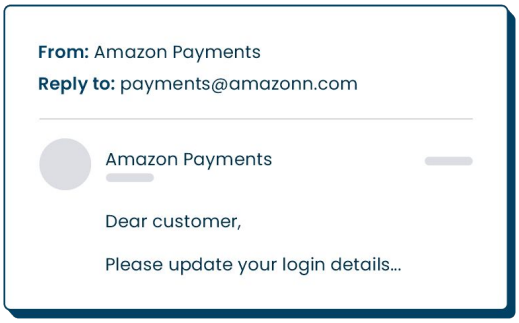
IronVest

Top 7 most common and most dangerous phishing attacks.

1. Impersonating a well-known organization's domain

Details: the email comes from "Amazon Payments" <payments@amazonn.com> or even "Amazon Payments" <payments@amazon.net>

How InboxGuard protects against this: NLP and AI are used to detect that a well-known domain is being spoofed



2. Impersonating a well-known organization's name

Details: the email comes from "Amazon Payments" <george@gmail.com>

How InboxGuard protects against this: NLP and AI are used to detect that a well-known company name is being spoofed and there is a mismatch between the company name and the domain

3. Impersonating your own domain

Details: say your company is "Acme Ltd" and your email address is "john@acme.com." In this case, the spoofed email will come from "John Smith" <john@acne.com>

How InboxGuard protects against this: the product detects that the sender name is similar to an employee and that possible impersonation is taking place

4. Impersonating your own organization's name

Details: say your company is "Acme Ltd" and your email address is "john@acme.com." In this case, the spoofed email will come from "Acme Ltd" <jane@gmail.com>

How InboxGuard protects against this: NLP and AI are used to detect that someone is trying to impersonate your company name

5. Impersonating an employee (including a CEO)

Details: say your CEO is John Smith. In this case, an email might come in from "John Smith" <johnsmith@gmail.com> saying that they are using their personal email as they're writing this quickly from the airplane before it takes off etc.

How InboxGuard protects against this: NLP and AI are used to detect that someone is trying to impersonate your company name

6. Hijacked domain

Details: an email is received from a new sender, that reminds you that your password is expiring. The sender is "Accounts Payable" <accounts@jennysflowers.com>. This is dangerous as the hijacked domain probably has all the major security credentials in place (DKIM, SPF, etc.)

How InboxGuard protects against this: the product detects when an email is a first-time sender, when there is phishing language used within the email, when there are malicious links in the email, etc.

7. Impossible-for-human-to-detect attack

Details: an email is received from "Amazon Customer Service" <support@amazon.com> and seems completely legitimate.

How InboxGuard protects against this: by observing the way that the email was sent, the servers it bounced through, the typical sending patterns of this sender, etc., InboxGuard can pick up that this email is not genuine.