Adversary In the Middle Cyberattack

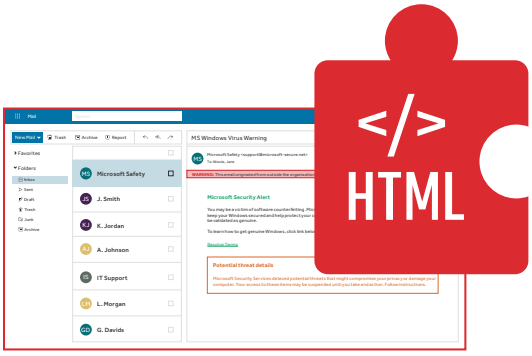
This is a common cyberattack technique where the adversary will intercept authentication information when an employee signs in. The adversary will then use that access to exploit the employee, the company, and even the company's business partners. Here's how it works...

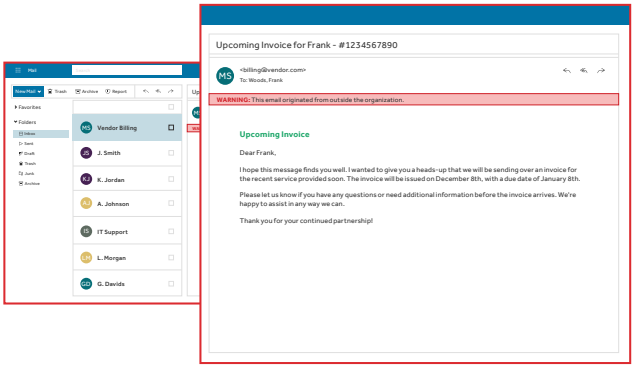
1 Frank, a dealership employee, clicks a phishing email and is directed to a proxy website and begins entering his credentials.

This simply means information entered into the proxy site is captured by the adversary before it is passed along to the real website.

2 The adversary captures Frank's credentials and signs into Frank's email. (Frank has no idea this has happened.)

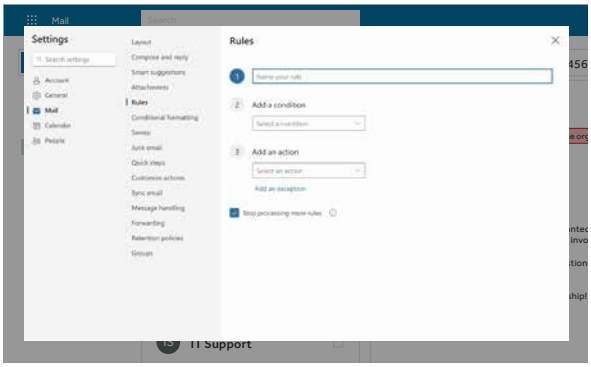
3 The adversary uses tools embedded with AI features that allow him to gather intelligence from Frank's email more quickly.





4 The adversary's AI tool finds an email conversation about an upcoming payment to an outside vendor and maps out the org structure of the dealership's accounting team.

5 The adversary sets up inbox rules to hide the conversation between the vendor and the adversary while it takes place in Frank's mailbox.



All of this has happened in the span of just 20 minutes. The adversary was able to build his attack playbook leading to financial fraud.

From: frank@dealership.com (aka the adversary)
To: billing@vendor.com

Can you send me a line item invoice? Also, can you resend the wiring instructions for the payment?

6 The adversary sends a message to the vendor asking for more information about the invoice. The adversary is just building plausibility to cover his own tracks.

7 The adversary intercepts the payment instructions and changes them to point to a bank account he owns. Then, he forwards the email to the accounts payable team to make the payment.

8 The adversary walks off with a nice payday. Frank gets a call from the vendor asking about the missing payment.

Once the adversary gains access, he can sift through your email, contacts, and cloud documents. Depending on the employee's role in the dealership they could redirect funds, steal money, and collect personal information. They could even launch a full-scale ransomware attack.

Ensure your dealership has the proper prevention, detection, and remediation mechanisms in place. Visit info.protontechs.com/account-shield or call 866.605.1027.

PROTON DEALERSHIP IT CYBERSECURITY