Staying Ahead of Cyber Threats: Lessons from a Recent Ransomware Attempt

On April 30, COMPANY successfully defended against a sophisticated ransomware attack. Just days later, an employee narrowly avoided falling victim to a spear phishing attempt while traveling. These back-to-back incidents underscore an important truth: no organization or individual is immune to today's evolving cyber threats.

Thanks to our proactive security investments and the quick actions of our people, both threats were stopped. Here's what happened, what we learned, and what you can do to stay protected.

The Ransomware Attempt

What Happened

A known ransomware group launched a targeted spear phishing campaign against our organization. Their approach included:

- Mailbombing select employees with unsolicited SPAM
- Impersonating internal IT support through email, phone, and Microsoft Teams
- Attempting remote access using a legitimate tool, Microsoft Quick Assist
- Contacting a targeted selection of employees with personalized messages

How It Was Detected

Our layered defenses performed as intended:

- Our Security Operations Center (SOC) identified suspicious activity and escalated immediately
- Our Security team investigated and isolated the affected endpoint within minutes
- Log analysis confirmed compromised credentials and triggered further containment actions

How We Responded

- Disabled Microsoft Quick Assist across the organization
- Blocked the IP addresses used in the attack

- Sent clear communications and guidance to all employees
- Rotated credentials and reinforced security measures

Outcome

- No data was lost
- No further malicious activity was found
- Business operations continued without interruption

The Evolving Tactics of Cybercriminals

These incidents highlight how cybercriminals are constantly evolving their craft. Some of the tactics used today include:

- Spear phishing with emails that look legitimate and are customized for the recipient
- Employing multi-channel deception through a combination of email, phone calls, and chat messages
- Misusing legitimate tools like Microsoft Quick Assist to gain access
- Social engineering our people to create urgency or confusion to encourage quick decisions

This is why having a layered defense made up of technology, processes, and people is so critical.

Real Story: Quick Thinking Prevents an Attack

EMPLOYEE was recently targeted by a convincing spear phishing attack while traveling.

Here is what happened:

- She received strange spam text messages
- When logging onto her laptop, she was hit with dozens of suspicious emails
- She then received a Microsoft Teams call from someone claiming to be IT support

Ann trusted her instincts. Rather than sharing credentials or allowing access, she:

- Asked the caller to verify their identity in writing

- Submitted a ticket through ServiceNow
- Contacted the Security team directly

Thanks to her quick thinking, the attack was stopped before any damage occurred.

Ann said, “The caller sounded completely professional. They knew the right things to say, but something felt off. I’m glad I trusted that instinct.”

This is an important reminder that cybercriminals can strike at any time and from anywhere.

How You Can Stay Safe

1. Report anything suspicious
   Use the Report Phishing button in Outlook
2. Never share credentials or grant access
   Always verify that you are speaking with legitimate IT support
3. Escalate immediately
   Submit a ticket in ServiceNow or contact IT Support through Teams
   IT Support will work with Security to investigate
4. Stay informed
   Read official updates from the Security team and share them with others

Final Thoughts

These events show that our layered approach to cybersecurity is working. They also serve as a powerful reminder that staying ahead of threats takes teamwork, awareness, and fast action.

If something feels off, speak up. Contact the Security team or your local IT Support representative anytime.

Together, we can protect our people, our data, and our business