HIGHER EDUCATION CASE STUDY

How a mid-sized community college used ConcealBrowse to lower their susceptibility and risk to ransomware

AT A GLANCE

A mid-size community college with approximately 3,000 faculty and staff and 70,000 students was experiencing high susceptibility among its users to phishing attacks, resulting in the execution of malware payloads and loss of credentials. Despite performing security awareness training for years, the college found that users in any group were susceptible to a range of scam techniques, and they operate on a limited budget.

RESULTS

Although it is still early in the deployment, the college has already seen a 25% reduction in endpoint alerts, and they have not received any user complaints. Furthermore, the solution has provided increased visibility on credential harvesting sites targeting their users, giving the college a more comprehensive and effective way to protect their users from phishing attacks and cyber threats.

25%
reduction in endpoint alerts

Zero
user complaints

CHALLENGE

Like others in higher education, the college was experiencing high susceptibility amongst its faculty, staff, and student populations to phishing attacks. These attacks were resulting in an increased threat to ransomware and harvesting credentials. They found that users were susceptible to a range of techniques beyond email, including social media sites, messaging applications and other applications. These additional attack vectors made it difficult to respond to, as their cybersecurity team was extremely limited. The institution needed a solution that could integrate with their existing security controls and neutralize attacks designed to their student and faculty credentials. Additionally, they did not want the solution to create false positive alerts that their small security team could not handle.

APPROACH

ConcealBrowse was easy to deploy, required no additional user training, and was affordable. It could integrate with existing security controls and neutralize attacks designed to execute a malware payload and those designed to harvest credentials. The solution was also designed to limit false positive alerts, which would have placed an additional burden on the college's small security team.

BENEFITS

1 Reduce Susceptibility to Phishing Attacks
ConcealBrowse helped the community college significantly reduce susceptibility to phishing attacks among their faculty, staff, and student populations.

2 Improve Visibility
ConcealBrowse provided increased visibility on credential harvesting sites targeting their users, allowing proactive measures to be taken to protect users from similar threats in the future.

3 Save Time and Money
The customer was able to save time and money by choosing a solution that was easy to deploy, required no additional user training, and was affordable.

CONCEALBrowse™
(706)-481-2642
conceal.io
info@conceal.io