PROTECTING AGAINST INSIDER RISK WITH CONCEALBROWSE

https://conceal.io/

INSIDER RISK

01

1,619 publicly disclosed cyberattacks on schools between 2016 and 2022

In the past year, ransomware significantly impacted the education sector, with 56% of lower and 64% of higher education institutions affected. The sector's vulnerability is attributed to inadequate cybersecurity investments and numerous devices accessing their networks, risking sensitive data.

02

Over 100 million patient records leaked in 2023

Recent research indicates a correlation between increasing ransomware breaches in the NHS, affecting over 100 million healthcare records in 2023 alone, and worsening patient outcomes, including fatalities.

WHY ADDRESS INSIDER RISK?

Insider risk remains a significant concern in cybersecurity, as evidenced by recent statistics. The 2023 Data Breach Investigations Report from Verizon highlights that human error is a factor in **74% of breaches**, emphasizing the challenge of mitigating insider risks.

2024 Threat Landscape

Phishing remains a dominant threat in the cyber landscape. IBM's 2023 statistics indicate that phishing was the leading infection vector, identified in **41% of incidents**, making it the most common initial attack vector.

Statistics

80%

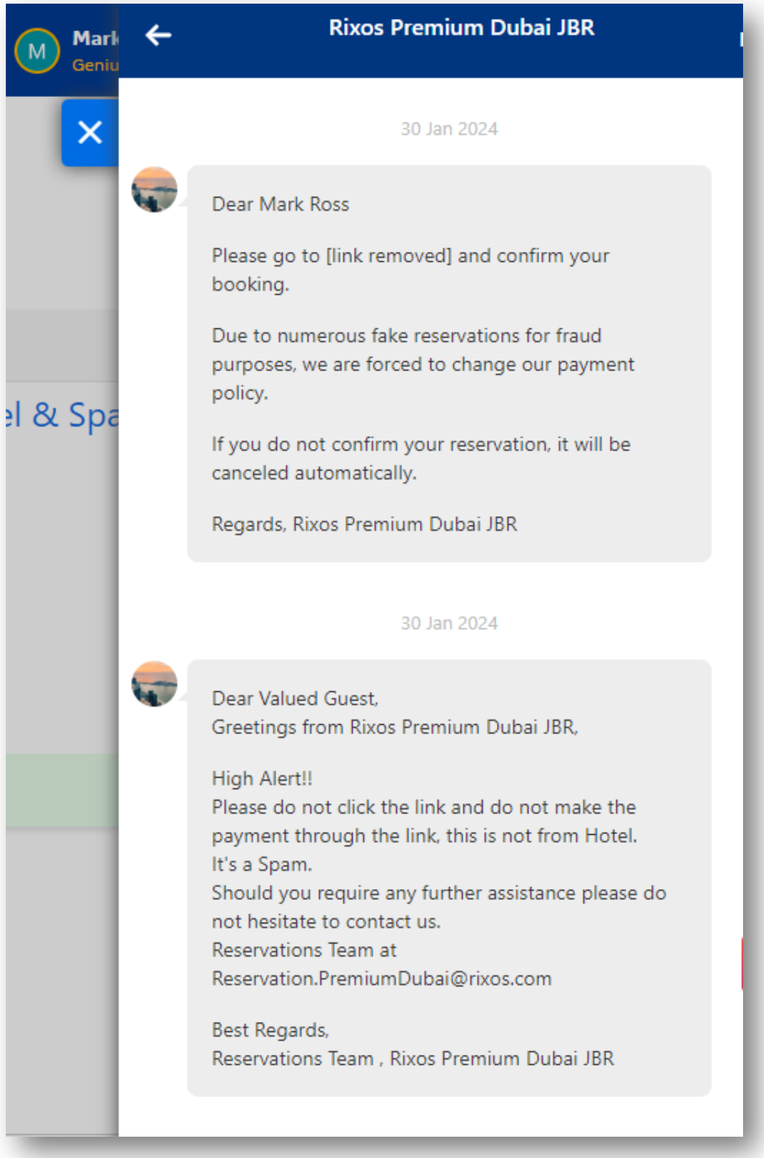
of reported security Incidents begin with a phishing attack

Statistics

$17,700

lost every minute due to phishing attacks

REAL WORLD EXAMPLE



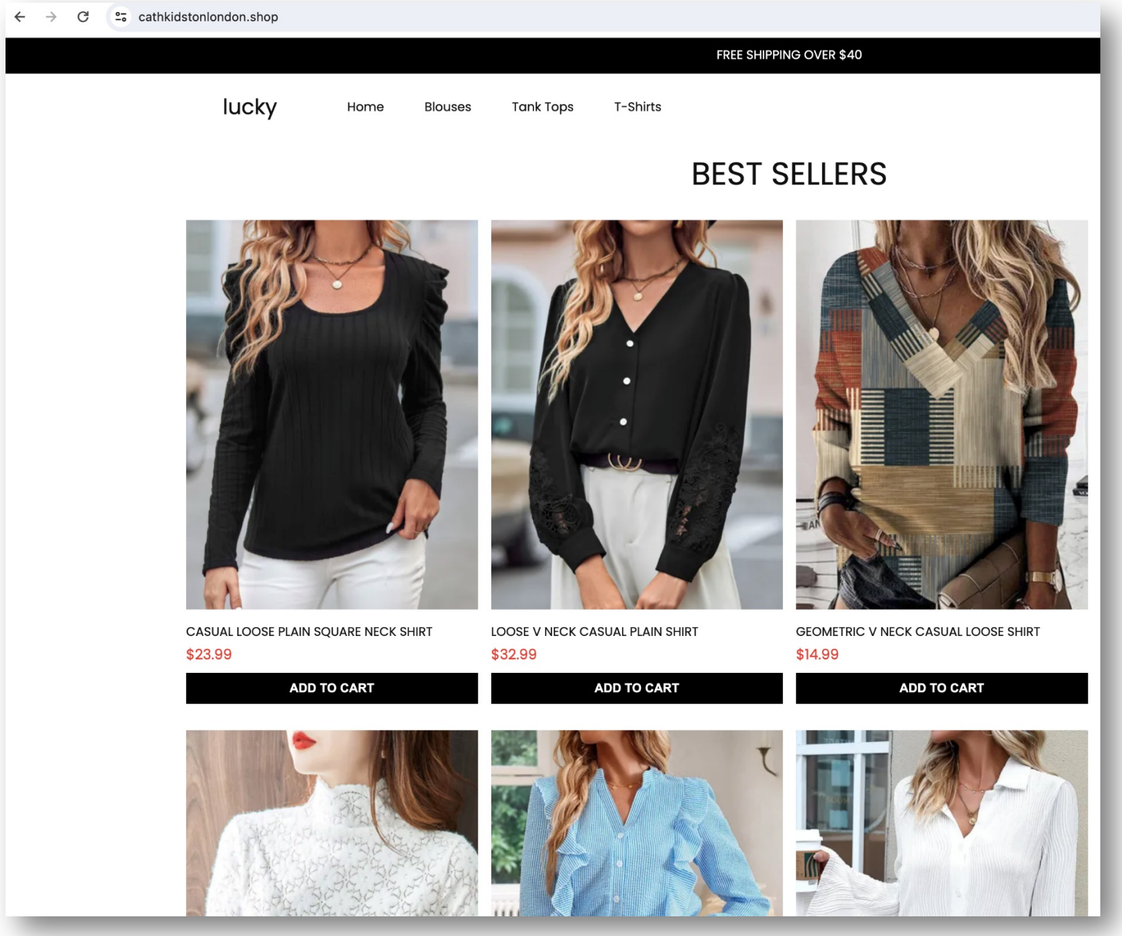
Received message to confirm booking and update credit card information

Clicked link to update booking

Conceal flagged the link as malicious

Planned to call Bookings.com in the morning, but when I returned to the page, learned the malicious link had been removed and there had been a follow up sent

EXAMPLE #2



Legit or Malicious?

Competitive prices, until site wouldn't let customer pay with Paypal

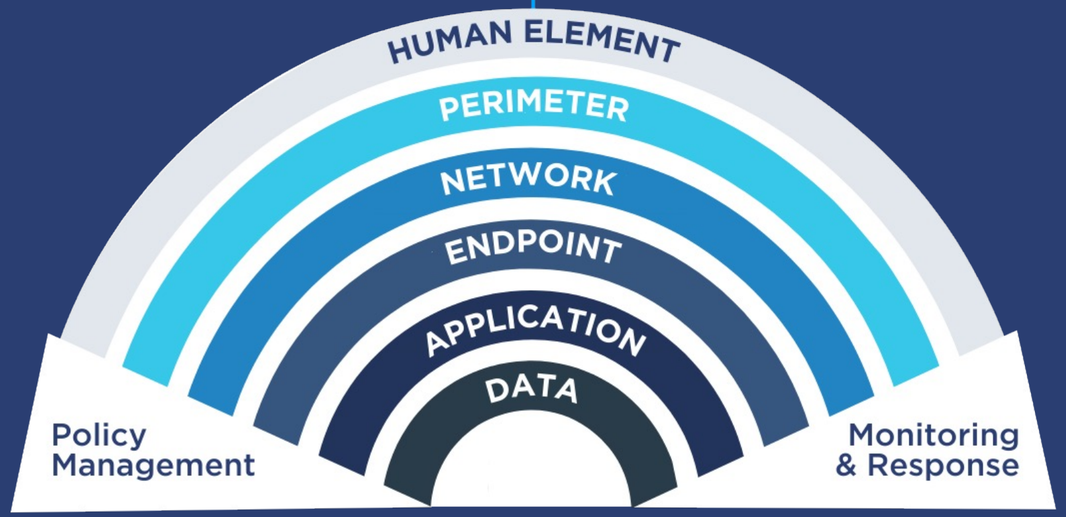
Opened in a ConcealBrowse enabled web-browser and it was blocked!

Synopsis: There was likely a link that was **malicious** that had been removed from the site so ConcealBrowse picked it up and it was safe.

Question is - would your average employer want this blocked? Even if it seems safe? That's not a decision you want AI making one way or another, so best to isolate…

MINIMIZING INSIDER RISK

Browser security can proactively protect against Insider risks originating on the edge



Access Control
Data Protection
Encryption
Remote Access

SIEM
File Integrity
IT Service Management
SOC
Identify Access Management
MDR

CONCEAL

A new control point securing the most vulnerable part of any organization - the human element

- Education, Training and Awareness
- Intrusion Prevention & Detection, NexGen Firewall
- Site-to-Site Connections, Web Filtering, Remote & VPN Services
- MFA, Endpoint Detection & Response, Patch Management, Antivirus
- Vulnerability Scanning, Application Whitelisting
- Data Encryption, Classification and Loss Prevention

ABOUT US

Step 01

A user navigates to a web page or clicks a link, and ConcealBrowse instantly analyzes the content to identify potential threats.

Step 03

Malicious or suspicious sites are quarantined or blocked, preventing harmful code from executing and blocking users from entering credentials.

Step 02

Without user interference, the SherpaAI engine evaluates & classifies sites as safe, suspicious, or malicious.

AI

browse
+SherpaAI

Every user interaction feeds back into the system, refining the SherpaAI algorithms - ensuring that the solution remains ahead of emerging and evolving threats.

INTERESTED?

Let’s chat! We look forward to connecting with you all during the networking session and lunch today.

Thank you.