Solution Brief

PREVENT CREDENTIAL THEFT

BLOCK CREDENTIAL THEFT ATTEMPTS FROM UNSAFE WEB SITES

SAFELY VIEW WEB SITES WITHOUT FEAR OF BREACH

ELIMINATE RESTRICTIVE IT SECURITY POLICIES THAT LIMIT USER ACCESS

STOLEN CREDENTIALS ARE THE KEY TO SUCCESSFUL BREACHES

Phishing attacks are the most common source of cybersecurity breaches in business today, and employee credentials are a top target for these malicious actors. That's because they are the key to unlocking many of the other security protocols put in place to protect your business. A correct user name and password combination is often all that stands between a cybercriminal and a company's valuable intellectual property.

Spear phishing is particularly effective because it often exploits a positive behavior – the person's desire to comply with security policies by providing or updating the very credentials that are supposed to keep them safe. It's also tricky to stop because malicious websites are numerous and short-lived. Their content changes frequently to avoid accurate categorization.

PHISHING REMAINS MOST COMMON AND EFFECTIVE CYBERTHREAT TO YOUR ORGANIZATION

Malicious phishing threats are constantly evolving and take many forms:

- Spear phishing: scams targeting individuals by including their names, roles, or work processes
- Whaling: aimed at company officers and often written as legal notices, customer complaints, or executive issues
- Social engineering: disguised as appeals to human nature's willingness to trust and be helpful
- Inadvertent infection: sharing news or social media links that have been compromised

Phishing attacks are executed in numerous ways:

- Phishing links in email messages
- Targeted links or messages on social media platforms
- Shared links in chat programs

HP SURE CLICK ENTERPRISE[1] HELPS PREVENT CREDENTIAL THEFT BY ALERTING AND BLOCKING USERS FROM SHARING LOGIN DETAILS ON MALICIOUS AND LOW-REPUTATION SITES

Sure Click Enterprise helps stop credential theft by preventing the ability to enter passwords on credential harvesting websites after a user has clicked on a phishing link in an email, chat client, PDF or other file. When a user visits a web site and is prompted to enter login credentials, Sure Click Enterprise utilizes the HP Threat Intelligence Service to conduct a reputation and domain analysis behind the scenes to determine the safety of the site. For legitimate, known safe sites, users will be free to enter their credentials as usual with no impediments from the software.

But if the site is a known phishing site, a warning window will appear over the page as the user attempts to enter their password, preventing the site from capturing their credentials. The software can be configured to then allow the user to either safely close the browser window, or proceed to view the site with all data-capture fields inactivated.

If a site has a low reputation, users are warned to check the site and avoid entering credentials unless it is a known safe site to the user. Administrators can choose to block credential entry to these sites, or allow users the freedom to proceed, which will then whitelist the site on that user's PC and remove the warning from future visits to increase prevent unneeded future productivity restrictions. All actions taken on known bad and low-reputation sites are recorded and reported to the Sure Click Controller for IT to review for threat and user behavior status.

CREDENTIAL PROTECTION: AVOID BREACHES FROM PHISHING SCAMS

Prevent Credential Theft from Phishing Attacks

Reduce the risk of employees being tricked by phishing scams. Sure Click Enterprise blocks users from entering login details on known malicious web sites, and alerts users to potentially risky behavior on all low-reputation sites.

Streamline IT Security and Reduce Costs

Drastically reduce triage time and stop wasting resources on false positives with HP Sure Click Enterprise's high-fidelity alerts. Eliminate reimaging, rebuilds, and emergency patching.

Share Real-time Threat Intelligence

Adaptive intelligence identifies and stops evasive attacks, shares real-time threat data across your network, and delivers full kill-chain analysis to your SOC.

Achieve Lasting Protection with Hardware-enforced Security

Only HP Sure Click Enterprise uses virtualization-based security to deliver hardware-enforced application isolation. Protect against unknown threats and polymorphic malware that easily slip past even the most advanced detection tools.

67%
of breaches are caused by credential theft.

- Verizon DBIR 2020[2]

Breaches involving stolen credentials cost global businesses an average of **$3.86 million per event**, and up to **$8.36 million in the US**.

- IBM Cost of a Data Breach Report 2020[3]

Learn more at https://www.hp.com/enterprisesecurity

1. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox and new Edge are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2020/
3. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

4AA7-8573ENW, October 2020, Rev 1