Sinclair
COPYWRITING

CYBERSHEATH
SERVICES INTERNATIONAL

WORK SAMPLE

CLIENT: CyberSheath Services International
PROJECT: Blog Posts on Cybersecurity (Credential Protection)

by Louise Sinclair | louise@sinclaircopywriting.com | www.sinclaircopywriting.com

HOW TO PREVENT CREDENTIAL THEFT

Sometimes, the simplest hacks are the most effective — and the most devastating.

Although password theft and email phishing seem like basic, run-of-the-mill cyber theft schemes that can be easily avoided, a recent Verizon Data Breach Report revealed that 81% of hacking-related breaches leveraged stolen or weak passwords to gain access to vulnerable systems.

This statistic is clear evidence that today's businesses are not taking the threat of credential theft seriously enough. And even though they're the most basic types of breaches, stolen credentials are profoundly effective, giving cybercriminals the ability to impersonate a valid user, bypass your entire security platform, and wreak havoc from within your systems.

If you don't want to fall victim to this highly avoidable scam, making sure you and your workforce understand the responsibilities of privileged access can ensure that your most sensitive data is properly protected.

Here are some simple steps to help prevent credential theft…

Understand how data is accessed

In the context of cybersecurity, "privilege" is a term used to describe special access or permissions above that of a standard user. Privileged accounts are required for administrators, applications, or devices to gain access to a system.

There are two main types of privileged access. The first is privileged access used by humans, such as domain administrative accounts, super-user accounts, secure socket shell (SSH) keys, or emergency accounts. These are accounts given based on credentials that only allow access to sensitive data to certain individuals.

The second type is non-human privileged access. This is typically an automated process, sometimes referred to as a "machine identity", which accesses your system independently to help simplify your day-to-day operations.

Examples of non-human privileged access may include applications that automatically pull data to help you stay organized, or "secrets", a catch-all term for application program interface (API) keys, SSH keys, or other credentials used by development and operations (DevOps) teams to give them automatic access while developing software.

Understanding the various ways in which data is being accessed gives you a better sense of where any gaps in your protection may lie. Take a look at your current situation and ask yourselves the following questions:

- What information of value do we have access to?
- How is it accessed and by whom?
- What protections are currently in place?
- Are these protections sufficient?

Know who's at risk

Certain high-level employees are bound to be targets for credential theft for obvious reasons — they rank highly in the company, for example, or they're IT professionals whose job requires them to access

every corner of your systems. However, there are other potential avenues for attack that might be less obvious.

If your company has board members, these non-employees make particularly attractive targets. They have high-level access but don't use company-issued hardware, and they might not have received proper security training, both of which can leave your company open to attack.

The fact that your board members are your most influential decision-makers can also be used to aid hackers in phishing scams. By impersonating a board member, hackers are more likely to convince other employees to respond to creative phishing baits and give them access to your systems.

It's not just people; some of your automated processes may also be in danger of being hacked if you're not keeping on top of them. Always download patches, maintain the latest version of your software, and never snooze those security updates!

Train and prevent

If you've found vulnerabilities in your cybersecurity strategy, waste no time in getting your staff up to speed with comprehensive training. A great start is to educate them on the latest phishing schemes to ensure they know what to look for.

You can also mandate that employees use multi-factor authentication, which requires that authorized users must successfully pass through several layers of verification in order to access privileged accounts.

Technology moves fast, so continue to invest in the latest tools and upgrades to stay ahead of threats. Continually refine your procedures and create audit trails that allow you to monitor privileged operations.

Get professional protection today

If you need a security strategy to defend your business from credential theft, let CyberSheath help. Our team of experts can provide you and your team with the tools, training, and guidance to keep your privileged information on lockdown. Contact us now to get started.

END OF SAMPLE

by Louise Sinclair | louise@sinclaircopywriting.com | www.sinclaircopywriting.com