Bloor

White Paper

White Paper by Bloor
Authors **Fran Howarth**
Publish date **July 2018**

Security is a human problem

People are the weakest link. But only lip service has been paid to this for too long. Technology is available to rectify this situation and every organisation should take note.

Summary

When it comes to security, humans are the weakest link. And the human problem in security is getting worse as traditional attacks become less effective owing to advances in the capabilities of security technologies.

The prime manner for exploiting human weaknesses is via phishing, which is now the cause of virtually all breaches that occur. Verizon has found that phishing drives 90% of cybersecurity breaches. Lures are still sent via email, but are becoming less effective as humans are taught to recognise them. Now, phishing attacks are moving in droves to web-based tactics, where users' guards are down, deploying all manner of techniques to target human weakness. Organisations are increasingly vulnerable and must evolve the way that they plan and implement their defences. A new approach is needed.

“Phishing attacks are moving in droves to web-based tactics, where users' guards are down, deploying all manner of techniques to target human weakness.”

How cybersecurity problems have evolved

Prior to the 1990s, cybersecurity was little discussed outside of specialist circles. But that changed. The first generation of cybersecurity attacks were generally more of a nuisance than a real danger. Some did cause harm, such as formatting disks or erasing files, and over time their ability to cause harm increased. The 1990s spawned the development of anti-virus controls that protected users from exploits that were already known about.

Over time, both the motivations for attackers and the sophistication of their exploits has changed dramatically. Financial gain from extortion and data theft that can be monetised, along with the pilfering of corporate assets such as intellectual property, are common motives for hackers who can be anything from professional gangs to nation states. Self-propagating worms, controlled by botnets under the control of hackers, were used to send spam, steal passwords and distribute other malware. These provided a taste of what was to come in the form of phishing campaigns. Identity-stealing programs became commonplace.

Technology vendors and providers did their best to keep pace—and in many cases they managed, causing traditional attacks to not only become less popular, but also less effective. Improvements made by vendors include more effective firewalls, advanced endpoint protection, two-factor authentication, and secure web and email gateways. Browsers are increasingly secure, security patches are being delivered faster and better coding practices are being used for applications. Insecure technologies such as Flash are barely supported any more, closing the security gaps that they enabled.

> **“Scammers go where users go. Social engineering is the biggest problem in cybersecurity today and occurs across all communications media. The web is the choke point and that is where defences should be placed.”**

Humans are proving to be the weakest link

As windows for direct attacks on networks and devices have been closing for hackers, they have been forced to turn their attention to new methods and techniques to achieve a greater likelihood that their attacks will be successful. Human error has long been a security issue, leading to technological errors such as vulnerabilities being introduced into software that could be exploited. But that is not the whole story. Humans are curious and often overly trusting. They can be socially engineered to perform acts such as giving away credentials, opening attachments that seem interesting but that are malicious, or clicking on tainted links. An attack method that is becoming more prevalent is to use ads and phishing pages to promote cool browser extensions that appear to victims to work as advertised, but that use keylogging to monitor and snoop, often leading to data exfiltration without a user's knowledge.

According to Webroot, 95% of web-based attacks now use social engineering to trick users. And the methods that they use are becoming increasingly sophisticated, in large part because users are increasingly trained to recognise security risks, as well as owing to improvements in network, application and browser security.

Phishing is one of the prime examples of how social engineering is used. The term was first coined in 1996, but by the mid-2000s phishers were riding on the wave of success following an upsurge of attacks on banks and their customers. The effectiveness of social engineering over automated exploits was proven.

Originally, emails were the preferred means of conducting phishing attacks since email is such a common communication method, often using malicious attachments or tainted links. But users are increasingly wary of such exploits and the number of users failing prey to email phishing is declining.

As well as this, the relentless pace of development in online communications has opened up other avenues of opportunity and has led to other sophisticated social engineering methods being developed. There are currently some four billion internet users and there are around 1.8 billion websites in existence. Social networking has become huge, including sites aimed at business professionals, and prove to be an effective means of communication for organisations and governments alike, including political parties. Mobile devices have made their use even easier by providing a more convenient interface for people to use whenever they want, wherever they are. All these factors are providing for greater interactivity—and greater reach for attackers looking to exploit human weaknesses.

Among the methods proving to be fruitful are ads, browser pop-ups, extensions and plug-ins, search sites such as Google, rogue apps, web freeware, chat applications and social media lures. Some attacks use content injection to turn legitimate websites malicious so users enter their personal information because they think they can be trusted, the use of search engines and social media feeds enables attackers to direct users to malicious sites, and link manipulation, malvertising and ransomware for extortion are becoming increasingly common.

Many browser-based attacks are written in HTML5 and JavaScript and execute entirely in memory. They are fileless from a malware perspective. According to the Ponemon Institute, 77% of attacks that successfully compromised organisations in 2017 utilised fileless techniques that have been specifically designed to evade detection and bypass the majority of endpoint security solutions. Further, it states that a third of all attacks that will be experienced during 2018 are projected to utilise fileless techniques. Whilst many services such as browser extensions do legitimate activities such as ad blocking or browser pop-up blocking, they are also able to perform malicious activity such as keylogging and data exfiltration. Web freeware and apps found in app stores can be turned malicious since fileless exploits can circumvent the efforts of vetters. This is especially true when exploits are designed to lay dormant for the normal testing period, or to only release their malicious payload after getting an in-app update.

> **If your organisation has been in existence for more than a few years, the probability of being hit by an insider-enabled attack is almost 100%.**
>
> **SANS Institute**

The inexorable rise of social engineering

> [In 2017], phishing attacks became more targeted and successful, and most phishing sites were only online for 4 to 8 hours.
>
> Webroot

As a result, social engineering is now the preferred and most prevalent method of attack. The figures speak for themselves. According to the SANS Institute, 80% of organisations have experienced a phishing attack and 46% of attacks were launched by users clicking on links in email. User error is an important factor, accounting for 48% of attacks that bypassed endpoint defences, but social engineering is a factor in a further 38% of attacks. SANS states that any organisation that has been in business for a few years can be almost 100% certain that they will be hit by an insider-enabled attack.

According to Verizon's 2018 data breach investigations report, phishing and pretexting, in which a person impersonates another, represent 98% of social incidents and 93% of breaches.

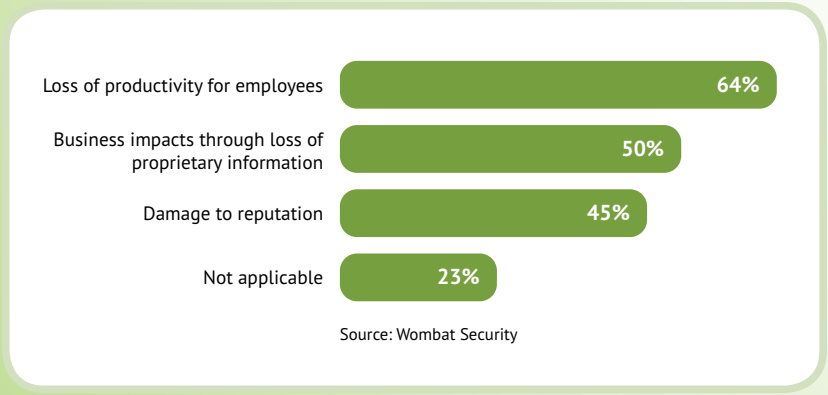

Figure 1 – How the cost of phishing can be measured

The use of phishing URLs is becoming increasingly common. Hackers can automate the registering of new domains and stand up hundreds, if not thousands of domains and pages in a quick, automated fashion. According to Webroot, 25% of all URLs seen in 2017 were malicious, suspicious or moderately risky, and there were an average of 1.4 million new malicious sites created every month. Such phishing sites are also often only live for a few hours before being taken down to avoid detection. Webroot found that most phishing sites were online for only four to eight hours.

It takes just one successful social engineering encounter to potentially cause a breach that can cost organisations dearly in terms of damaged reputations and financial losses through lost sales and possible fines. The FBI estimates that phishing schemes caused losses of around $1.6 billion from October 2013 to December 2016 among US businesses that it investigated alone. And those losses are mounting fast, with growth of 2,370% in the dollar amount lost seen from January 2015 to December 2016. Yet Verizon estimates that only 17% of phishing campaigns are ever reported. *Figure 1* shows the ways in which the damage caused by phishing attacks can be measured.

Traditional security controls proving to be ineffective

Traditional technologies used to safeguard organisations against the threats that they face are not sufficient to guard against today's sophisticated attacks that prey on human nature.

The problem is that many traditional technologies such as antivirus controls, sandboxes and even next-generation firewalls were designed to protect against attacks directly targeting the network, such as detecting the use of malicious binaries and web exploits. But attackers have moved on and are now targeting users directly, looking to exploit human weaknesses.

They are using a wide range of techniques that cannot be identified by traditional security controls, which are often based on static rules such as signatures and sandbox rules. Many of the attacks being seen today bypass such defences because they do not rely on files such as attachments. Rather, hackers are looking to trick victims into actions that will help them gain access to their devices and/or the network.

“Attackers have moved on and are now targeting users directly, looking to exploit human weaknesses.”

What is needed

A different strategy is required to deal with threats directly targeting employees via the web by detecting and blocking such exploits from impacting users. What is needed to protect against phishing attacks is a combination of email phishing protection, email gateways, URL filtration via secure web gateways, live phishing detection and phishing training.

Static signatures and rules are insufficient. Since the attacks being seen today do not require the use of files to deliver their payload, but rather use web-based methods disguised as innocent web traffic, attacks simply bypass multilayered security defences. Because attacks increasingly rely on web delivery, the web is the point where those attacks must be stopped. To deal with fast-changing, malicious URLs, a new approach is required. Static blacklists have no way of keeping up with the problem. Rather, technology is required that can perform real-time analysis of new sites and can send signals to firewalls or a DNS server to block a malicious URL.

Because the attacks being seen target human nature, a system is required that can take human actions into account. Humans have the ability to visually inspect things, read text, apply context to a situation, and learn from experience by remembering what has happened in the past. To beat social engineering attacks, the security controls used must mimic this behaviour, replicating the capabilities of human intuition. It must be capable of analysing, predicting and blocking cyber threats through self-learning capabilities, honed through analysis of millions of phishing and benign attacks so that it can determine whether the behaviour being seen is malicious or not. If something is suspicious, it can be blocked before it can impact a user, and therefore the network.

> **“To deal with fast-changing, malicious URLs, a new approach is required.”**

Bottom line

Human nature is a key vulnerability and attackers know how to exploit it. People are the weakest link. But only lip service has been paid to this for too long. Technology is available to rectify this situation and every organisation should take note.

FURTHER INFORMATION
Further information about this subject is available from
www.bloorresearch.com/update/2382

About the author

FRAN HOWARTH
Practice Leader / Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of Mutable business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

Tel: **+44 (0)20 7043 9750**
Web: **www.bloorresearch.com**
Email: **info@Bloor.eu**