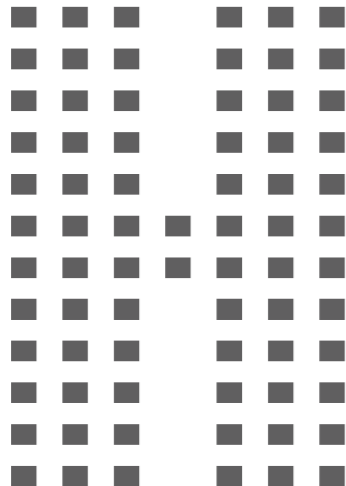


Michael Robertson X COMMERCE MEDIA X MANAGING DIRECTOR

Now it's personal

Protecting egamers from criminals is vital, and with cost-effective and simple software to guard personal data readily available, Commerce Media's Michael Robertson argues that users shouldn't be open to attack



THE THEFT OF EGAMING accounts has become a multi-million pound industry. Whether hijacking an Xbox Live or bingo account, the intent of online fraudsters is the same: to steal gamers' identities and credit card details and use them to either raid a gamer's bank account, buy goods illegally or sell the information on.

With any scenario, the impact on the gamer financially and emotionally can be devastating, and is potentially a complex and time-consuming situation to resolve.

For the egaming providers, any illegal activity going on via their network can result in brand reputations being damaged and financial losses if the activity becomes widespread, or if

users believe not enough is being done to protect their personal information.

A vulnerable sector

With the whirlwind pace of software development and broadband speeds, high-level online security for financial transactions is paramount.

The banking industry – which traditionally bears the brunt of online fraud – is one sector which has invested heavily in raising consumer awareness and updating its older computer systems to ensure the highest possible protection. It understands that installing effective security for web applications – and being seen to be doing so – has never been more important.

However, as such high-risk industries meet the fraudsters head-on, other, less secured markets are now seen as 'softer' targets. And as egaming continues to offer exciting, innovative and engaging content to attract more and more egamers, its appeal to malicious attackers intensifies.

Tools of the trade

Drawn by the sheer volume of egaming traffic and the sensitive nature of information shared between parties, fraudsters have developed evermore sophisticated methods to infiltrate online communities and access secure data through a variety of spurious techniques.

Phishing, pharming and trojan horse attacks are prime examples of ways to steal private data. The first two methods direct gamers to fake websites, either through an email request for information or automatically redirecting web traffic by corrupting a victim's computer or con-

sole. This is achieved by changing a host file or exploiting the vulnerability in the Domain Name System server; or software which translates internet domain names into their real addresses. In both cases, the victim thinks they are using a secure gaming website when in fact their details are being stolen by a third party.

Trojan horse crimes are more invasive and sophisticated as they take over the egamers entire hard drive. This happens when corrupted files – disguised as a screensaver, software upgrade or a new game – are downloaded by the gamer but then execute a malicious code that gives the fraudster complete control over the computer or console, while still displaying information the gamer will expect to see.

Both pharming and trojan horses are also known as 'man-in-the-middle' attacks, as a third party can intercept a legitimate exchange and modify information in real time before passing it on to its intended recipient. For example, in an online betting scenario, details such as where winnings should be sent can be changed and the player or the gaming provider are none the wiser.

Fighting the fraudsters

The techniques used by criminals are sophisticated enough that it's just as hard for organisations to know if a gamer's identity is real as it is for users to be certain that they are dealing with an authentic website or trusted network. As such, the traditional protection of 'name-and-password' authentication is no longer viable. So extra layers of personal security are a must to protect users – however, providers must consider the cost and simplicity of implementation, and, above all, make the security convenient and easy enough for users to use.



A two-factor approach

One method adapted from the financial sector is the two-factor authentication (2FA), a security measure in which the user must know something – a password or a pass-phrase – and must possess something – a token or log-in – to authenticate themselves.

In most 2FA applications, 'possession' is demonstrated by having a one-time-password (OTP) – generated either by a token

or at an initial log-in phase by the website's server – that is communicated to the user via a device such as a mobile phone.

As the name suggests, this password can only be used once, in real time. So using an OTP negates the possibility of a long-term password being lost, forgotten, or stolen via a phishing attack and then used to illegally access a gaming account later on.

The security of this solution is further strengthened by the fact that the OTP is

communicated by an independent medium and not the web, and has to be inputted by the gamer before an operation is verified. This makes it almost impossible for a 'man-in-the-middle' attack to succeed.

Another key benefit is that no additional hardware needs to be purchased or deployed, therefore reducing the cost of implementing 2FA.

As well as protecting an egamer, the 2FA can also offer added marketing solutions. For example, a promotional text message that links to a special offer or product announcement can be communicated at the same time as an OTP, without an additional charge.

Future fraud

The continuing rise of egaming crime is not surprising, but the lack of 2FA solutions being implemented is.

The technology is now relatively cheap to implement, and can offer a simple and convenient way to protect egamers.

Most important, however, is it will demonstrate an organisation's commitment to protecting its customers from the ever-increasing malicious attacks. ❖

As egaming continues to offer engaging content to attract more gamers, its appeal to malicious attackers intensifies

Michael Robertson