it's Firefox, Chrome, Internet Explorer, Safari or Edge. Most JavaScript is fine and makes web pages more interactive and responsive. However, JavaScript can also be malicious.

"Think about every ad that displays an animation designed to get your attention – it's running some code on your computer. Is it 100% safe? There's no way to know"

The same is true of embedded advertisements. An ad, purchased on a media website such as YouTube, is most likely legitimate – or it could be a front for malware that runs on the user's computer, even if the user didn't click on it. Think about every ad that displays an animation designed to get your attention – it's running some code on your computer. Is it 100% safe? There's no way to know.[2] Modern browsers do a pretty good job of keeping ads from gaining access to files on your computer or network, or from installing malware, but those ads can still use up memory and processor time to mine coins. What's more, if the employee clicks on them, the ad might try to install malware.

A challenge here is that your employee might not be doing anything wrong. While malicious ads are common on unsavoury websites (most notoriously on pornography sites), they also appear on what should be trusted, genuine websites. According to one researcher, this so-called crypto-jacking software was found on nearly 2,500 e-commerce websites.[3] And IBM's X-Force security team has documented the use of coin-mining software hidden inside web servers running Joomla or WordPress content engines, which can use the website visitor's website to mine coins.[4]

Never-ending battle

As with all malware and cyber-security, we're playing a game of whack-a-mole. Fix one problem, another pops up. Fix that problem, and oh, look, now there's coin-mining and coin-stealing. Be aware of the coin issue and foster a culture of security. We have beaten other security epidemics and we'll get this one too. And then, of course, we'll need to find the next pop-up mole that needs to be whacked.

About the author

Jesse Sampson, Ziften's director of analytics, brings to bear years of experience applying a variety of analytic methods – from traditional econometric analysis to modern machine learning techniques – across diverse industries. As a data scientist, he has made data do useful things for customers, stakeholders and partners in health care at 21CT, in workforce and education at the Texas Workforce Commission, and public relations at top Austin consultancy Vianovo before finally finding a new passion in cyber-security at Ziften. He has also delivered results as an analytics consultant for major companies in air transportation and logistics. Sampson holds a bachelor's degree in international relations and Chinese from Kalamazoo College and a master's in public policy analysis from the LBJ School at The University of Texas at Austin.

References

1. Schroeder, Stan. 'Crypto-currency exchange EtherDelta got replaced with a fake site that steals your money'. Mashable, 21 Dec 2017. Accessed Mar 2018. https://mashable.com/2017/12/21/etherdelta-hacked/#n30pOLGPbqqM.
2. Goodin, Dan. 'Now even YouTube serves ads with CPU-draining crypto-currency miners'. Ars Technica, 26 Jan 2018. Accessed Mar 2018. https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-crypto-currency-miners/.
3. 'Cryptojacking found on 2496 online stores'. Gwillem's Lab, 7 Nov 2018. Accessed Mar 2018. https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores/.
4. McMillen, Dave. 'Network attacks containing crypto-currency CPU mining tools grow sixfold'. SecurityIntelligence, IBM, 19 Sep 2017. Accessed Mar 2018. https://securityintelligence.com/network-attacks-containing-crypto-currency-cpu-mining-tools-grow-sixfold/.

Making information security easier

Luke Briner, PixelPin

Luke Briner

For too many people, information security makes their head hurt. At best we can keep a light grip on a small part of the risk base, but at worst it feels like trying to climb a greasy pole. For every strong movement upwards we end up feeling like we know less than we did before. How is that possible? Just like being a doctor, lawyer or tightrope walker, working in information security is hard. Very hard.

There is a perception in the general workforce and public that information security is basically some paperwork and a few pieces of hardware, a bit like fitting a burglar alarm to your house. How hard can it be? How on earth could TalkTalk, Equifax, Sony and all those other breached companies fail their customers so badly?

"A designer might be able to produce good designs without formal education but can we really carry on allowing just anyone to set up a 'web design company' writing production systems that are storing user data, processing card transactions and so on?"

Hopefully, all of us know that despite some mistakes made by these companies, most of us could have been in the same position – perhaps some of us already are. So let's discuss some of the reasons why information security is difficult and, by taking a step backwards, give some suggestions about ways in which things must change if we are ever to move away from a reactionary industry to an effective and proactive one.

Large arena

Information security (IS) is a very large arena. Currently, most IS professionals are expected to be experts in everything; but that's like thinking that all engineers are experts in electrical, mechanical, chemical and civil engineering. I am an electrical engineer and know precisely nothing about civil and chemical engineering. Why would I?

In the IS world, however, what we have not done effectively as a profession is to clearly segment areas of expertise so that you can be, for example, a 'network security manager', where that means something specific like 'electrical engineer'. There are some elements of this within certain organisations but these are not defined roles and can end up crossing over. Is the network manager in charge of security on our web applications? Just the network bits? Is that the role instead of the application security engineer? Like most things, having something to begin with, even if not perfect, is better than being entirely ad hoc.

One problem you see frequently is the lack of formal education or qualifications required to enter the world of digital. Sure, a designer might be able to produce good designs without formal education (even if it would still help) but can we really carry on allowing just anyone to set up a 'web design company' writing production systems that are storing user data, processing card transactions and so on?

An example encountered recently is that of a system a colleague saw that is still in use at airports and which could be used trivially to dump information onto TV screens such as bomb hoaxes or other inappropriate content. Why is it easy to hack? Because it was written by people who didn't really know what they were doing. It's not uncommon for developers to know virtually nothing about web application security. Does training guarantee they would know more? No, but it would certainly put things on the radar for most organisations, since a single person is all it takes to bring something good to the wider team.

"Should we insist that a company is not allowed to write applications that store personal data, operate on safety-critical systems or sit alongside those that do unless they have an appropriate certification?"

At least at management level, most people will have an accreditation, but should this be a legal requirement if we are to take the trade seriously? We would be mortified to hear that a doctor operating on us was not qualified because, 'they taught themselves and know roughly what they are doing'. For some reason, this has happened to our industry and we need to improve things: even if we can only directly affect our own company initially, we probably need to lobby governments to regulate the industry more, at least within certain parameters.

Training and education

The world of training and education also needs to get involved. We already have accredited courses. If you want to be a chartered engineer, a doctor, a lawyer or accountant, you have to pass certain exams after doing specific training. These are maintained by the industry and government departments to ensure standards are upheld – but in our industry, not so much.

Should we have accredited diplomas, degrees etc? Should we insist that a company is not allowed to write applications that store personal data, operate on safety-critical systems or sit alongside those that do unless they have an appropriate certification or the project is signed off by someone with one? Could we not require that the head of IS in an organisation must have an accredited qualification but also team leaders, design authorities, even the 'chief application security officer' who could be the one who is in charge of application security legally and must have an accredited qualification?

Of course, some in the industry would complain that it is hard enough to recruit as it is, let alone with this requirement. That cannot be an excuse, however, for not fixing something that is broken. Again, the trick would be to do something now that at least fixes part of the system and improves it as the industry has time to adjust.

Ad hoc environment

Managing information, sorting the old from the new, the good from the bad, the relevant from the irrelevant is basically impossible in the current ad hoc environment we work in. Take an example: if you want to understand GDPR2 regulations and do a Google search, you will get 5.7 million results. In this case, the top results look promising – the EU site and the UK site, followed by Wikipedia and a lot of other people trying to be helpful. Why so much information? Because if you write a helpful article on GDPR, people might come to your site and buy your legal services or invite you to a conference or maybe you will get ad revenue. Alternatively, perhaps the official sources are far too terse and impenetrable for us mortals to understand.

This problem exists in some domains much more than others. Search for a programming problem and you will get thousands of hits, some of which you do not know are relevant, some might be good or even good *if* you are doing it in a certain way. Maybe it used to be a good way but not any more. It seems there is no general movement to sanitise and score the information that we are trying to use to do things properly – everyday questions, especially for newbies, such as regulation, industry best-practice, new technologies, software vulnerabilities and so on. How many of you know whether you are running vulnerable software like Equifax was?

> ***"It seems there is no general movement to sanitise and score the information that we are trying to use to do things properly – everyday questions, especially for newbies, such as regulation, industry best-practice, new technologies, software vulnerabilities and so on"***

The current 'best' solution is that someone comes along and thinks they could aggregate the data for us to use. Which is great, unless they are also pulling in bad data and not following updating advice, as well as the fact that multiple people always attempt to fix the same thing. Want advice on ISO27001? Good luck. This is a much harder problem to solve, of course. The information does not belong to any one person, although the search engines could potentially do something with listings to help us find what we need.

What we really need is a creative solution – something different. Rather than trying to reorganise the mess, how do we rethink it? How do we get governments, industry bodies and so on to recognise that people need several different formats of the same information – the newbies' guide, the outline, the cheat-sheet and the full-blooded lawyer-pleasing regulation? Perhaps if these were produced well, the demand for these other unsolicited 'help guides' would diminish. We need to get the authors of these help guides to provide metadata that helps the search results to expire or to correctly categorise information rather than the web 1.0 'trick' of trying to put it into as many categories as possible.

Legal regulations

One of the areas that is discussed frequently, especially after a major breach, is the role of legal regulations. How can countries legislate to protect people from poor security? Unfortunately, with the current state of information security as discussed above, the answer is, 'not very easily'. Could Equifax *theoretically* have dealt with the known vulnerability in its web application and prevented the breach? Yes. Was it criminally negligent in not doing so? Probably not – in the same way that most of us would not be happy about ending up in court because our Windows 10 machines were not up to date and some CPU bug was leveraged for an attack and we 'knew about it'.

There is also a problem about borders, which are more easily respected in legislation than they are in the digital world. The Pirate Bay used the lack of copyright laws in Sweden to avoid the US authorities. And even if it was breaking laws, all it would need to do is to locate somewhere where enforcement is hard or expensive and it could continue to do things on the cheap and without the protection that could be offered by a law.

That isn't to say that a government couldn't introduce some kind of accreditation like we have for window installers or gas fitters. This would be a badge that effectively says, 'you could theoretically go to someone else but if you did you would not be insured and would potentially be committing a crime'. Perhaps that would be a way to push suppliers into taking their craft more seriously. Potentially, this badge could be acquired by a web application framework or piece of vendor hardware so that if used in accordance with instructions, you are automatically covered. Only if you start customising it or modifying it outside of known parameters would you be liable for ensuring that your own staff had the relevant qualifications.

What can the industry do? What can our companies do? What can the industry organisations do? To start with, we need to be cautious about reinventing the wheel and creating something else to throw into the large pot of information we already cannot handle. In a famous cartoon there are 14 competing standards and someone says, "It is ridiculous that we have so many – we could create a single universal standard to replace them". What happens? You end up with 15 competing standards.

Any new work should be co-ordinated at as high a level as possible. Contact one of the industry bodies or your local government representative. Talk about the problem. Is your solution a good idea? If so, can it be done in a publicly visible way so others know that you are already solving the problem? You might be surprised at what is already happening but which you simply can't see.

At the coal face

What can you do? You and your team might be the lowest level operatives. You are going to see the coal face with all its challenges and horrors but you are not usually placed in a position of enough authority to directly improve things. The best advice is to learn to step back, something that not all engineers and managers are good at. Is the problem that there is competing advice for GDPR or is the bigger problem that knowing generally what is and isn't true is difficult? Solve the second and you might solve the first. Learn what is foundational and what is noise.

If you find it hard to configure a piece of XYZ equipment, that is not a high-level information security problem that needs solving. If the problem, instead, is that configuring *all* types of network equipment is hard, expensive or error-prone then maybe there is a general problem that needs solving by the manufacturers.

> ***"Software as a service is great for many reasons – it can be maintained and updated in a single place and it can be scaled for higher numbers of users more easily than a hosted system"***

Make sure you play nice with one another. A manager's problems are not a worker's problems but that doesn't mean you have to argue about it. Communicate so that the worker knows that, for example, you are under pressure to deliver because a customer is threatening to go somewhere else, rather than saying 'just get it done'. You might be surprised that some of your workers come up with creative solutions if they know what they are trying to achieve. Likewise, if you are a worker and your manager is telling you to do something, by all means politely question whether X is better than Y; but if you tell them the risks and they still do what they want to do, that is on them – don't make it a problem, you need a good team in the proactive and reactive phases of IS and the last thing you need is bad feeling among the team.

What many newer industries lack are creative solutions. There are some areas where things have been generally modernised. For example, software as a service has delivered robust solutions to many companies in areas of customer relationship management, accounting, HR and others. Software as a service is great for many reasons – it can be maintained and updated in a single place and it can be scaled for higher numbers of users more easily than a hosted system. Now that most parts of at least the developed world have 24-hour Internet access, it is no longer unacceptable to have a system that requires a working Internet connection in order to be used. But as good as those improvements are, they are really an evolution of what already existed and since the light bulb was not invented by continuous improvements of the candle we need to encourage more lateral solutions to the things we struggle with. So let's look briefly at two such ideas and the problems they solve.

Hiding email

The first idea is that we can easily hide email addresses from companies who abuse the information by being overly presumptuous about how many emails they can send you (and sometimes the unsubscribe links mysteriously don't work) or where their business model is to sell the information to others who will send you a ton of marketing information. Conferences can be great, but these are another route for your email address to get to more people than you can control.

There are authentication as a service offerings that use pictures instead of passwords and these can provide a mechanism that does not provide an email address to the organisation when a user logs in but instead provides an opaque key – basically a randomly generated number.

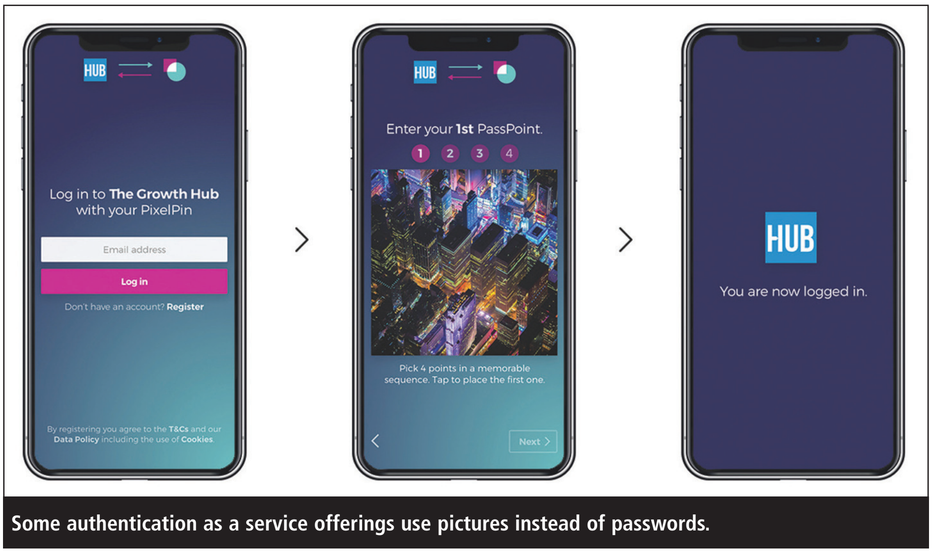
The only way for the company to contact the user is to use the service supplier's API endpoint, authenticate as themselves and send the message with the opaque key. This way, not only can the system hide the email address of the end user from the company, it can also track who is really sending emails (if the sender is not obvious from the content).

> ***"One of the things that shocked most people about Equifax was not that it was breached but that this company, that most people had never heard of, had their private information – lots of it"***

The user can report anyone abusing the sending of emails and the service can easily revoke access either for the company or for a specific user to prevent abuses. Passing this token onto another company will not work unless you also pass your authentication credentials, which could work, except the first company would still be seen as the source of the unsolicited emails and could be sanctioned.

The over-sharing problem

The second idea is to solve the problem of over-sharing private data and thereby increasing the risk of data theft. One



Log in to **The Growth Hub** with your PixelPin

Don't have an account? **Register**

By registering you agree to the **T&Cs** and our **Data Policy** including the use of **Cookies**.

Enter your **1st** PassPoint.

Pick 4 points in a memorable sequence. Tap to place the first one.

You are now logged in.

Some authentication as a service offerings use pictures instead of passwords.

of the things that shocked most people about Equifax was not that it was breached but that this company, that most people had never heard of, had their private information – lots of it. How does it happen?

Institutions that lend you money or provide credit want to know whether you are a reliable customer. They do this by passing the details they collect from you to a credit agency that does this on behalf of so many other institutions that between them they can provide some assurance as to whether you should or should not be lent money. What actually happens is that a company can pay these credit agencies to send them your data – about other borrowing, about address history; it's a large dataset. Even if you don't have a relationship with the end user, you can still buy this data.

The reasoning is sound enough, it is just the implementation that is very risky. We trust institutions like banks not to lose data but it is certainly not guaranteed that it is safe. And if it was stolen, would you know? If you don't like this arrangement then don't borrow anything – no credit cards, no mortgages, no loans and no mobile phones. This is basically not an option for most of us.

So how do we provide the needed outcome without the risk of data sharing? The solution is something we call 'inversion of responsibility' or 'inversion of control'. Rather than an organisation asking the credit agency to send it all of your information, it instead sends the credit agency the lending 'rule' that it will run on the data. The credit agency runs the rule itself and returns the result to the organisation without the latter ever having to see any private data.

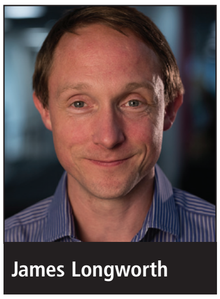
This solution wouldn't have helped with the Equifax breach but if far fewer organisations need to see the private data, the risk of it being stolen is massively reduced. The same basic principle could and should be used with authentication as a service where, instead of collecting customer data yourself, you trust a specialist company to do it for you. It provides the information during a session, so you can get delivery addresses and so on. But as soon as the customer logs out, the information is deleted or anonymised and your risk is removed.

Perhaps you have other ideas? Make them happen, make sure they live in the correct domain – industry, legal, corporate – and let's try and make our industry slightly less hard.

About the author

Cyber-security expert Luke Briner has a strong white-hat hacker pedigree and a passion for electronics. CISSP certified with special expertise in software security, he is the CTO at PixelPin, a company that offers a personalised two-factor visual authentication solution.

VPN: from an obscure network to a widespread solution



James Longworth

James Longworth, Insight UK

Looking at the evolution of virtual private networks (VPNs), one can see a clear shift in their usage in the past decade or so. While VPNs used to be reserved for big companies and government authorities – proving a mystery or unjustifiable expense to most – today we see VPNs being implemented and talked about on a much wider scale. From organisations of all sizes to individuals, more and more people are turning to VPNs to safeguard their data and ensure privacy.

However, to understand what key benefits this technology provides its users, we must first look at how it works. In short, VPNs are used to protect data from being accessed or altered as it travels over another network (eg, the Internet). This is possible through the use of a wide variety of computer protocols that securely 'wrap' your data in a layer of encryption and ensure that the destination for that encrypted data is authenticated (ie: the person or system is who it says it is) and authorised (allowed) to 'unwrap' it. In other words, VPNs allow users to securely access a private network and also share data remotely.

The rise of VPNs

The rise of VPNs goes hand in hand with the rise of other technologies that require a higher level of cyber-security protection. For instance, the sudden rise in popularity of virtual private networks and their current ubiquity is down, in part, to the rise of technology trends such as the Internet of Things (IoT) and bring your own device (BYOD), as well as legislative changes that allow state bodies to require ISPs to monitor and log individuals' online activity.

With more and more entities using these technologies on a daily basis, an increasingly larger number of individuals and organisations have begun to turn their thoughts towards the benefits of VPNs.