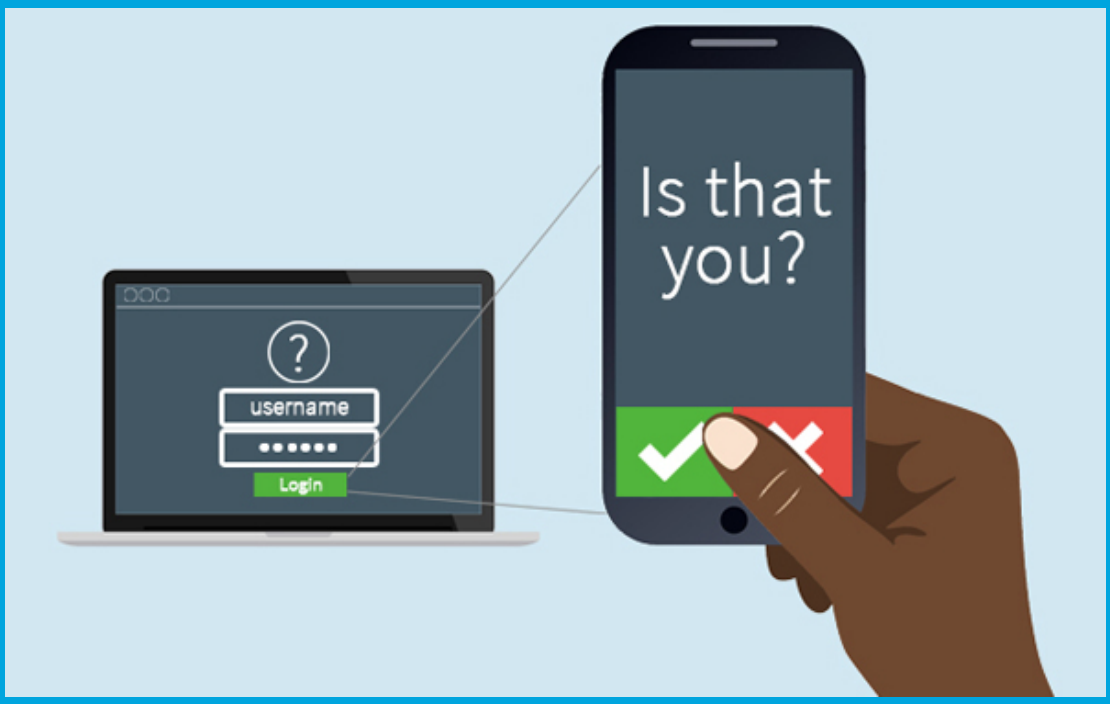
kindred

Security Newsletter

2 May 2017

2-Factor Authentication is great, but it's not a silver bullet



This week's featured article is more like a featured topic: Two-factor authentication, or 2FA. 2FA is getting more and more common, and it's great, but we think it's important to remember than it is not the silver bullet of secure authentication. 2FA can be bypassed, either by a flaw or by design, and phishers are getting better at bypassing it.

2FA can be badly implemented, resulting in the authentication system being no stronger than classic, password-based login. This is what happened with LastPass recently, which stored the 2FA secret seed under a URL that could be derived from your master password. While this URL needed authentication to be accessed, and the content of the querystring was protected by HTTPS, it was possible to get it by forcing the target to make the request for us using Cross-Site Request Forgery (CSRF). Thankfully, this is now fixed.

Please also remember that you often have ways to login without 2FA, this is generally the case for API or third-party application accesses. The Russian hacking group blamed for

targeting U.S. and European elections has been breaking into email accounts levering this fact. They sent fake emails, pretending to be from Google and suggests users install a security app called “Google Defender.” However, the application was actually a ruse which duped users into giving up a special access token for their Google account, known as an OAuth token. OAuth tokens car provide long-living, stealth backdoor to your account, and often reseting your password won't even revoke this access.

Finally, a lot of services enforcing 2FA allow you to "remember this device for X days", so that they conveniently just ask for your password for a month after you've logged in once using 2FA. This can be leveraged by phishing websites, which will act as a proxy between you and the targeted service. They will ask for your password (and steal it), pass it back to the target site to login, then forward you the request for the second factor. Once fully logged in, they will keep the "remember me" cookie so they can log whenever they want, just using your (stolen) password. Some tools, such as Evilginx, even allows to automate this for popular targets, such as Google or Facebook.

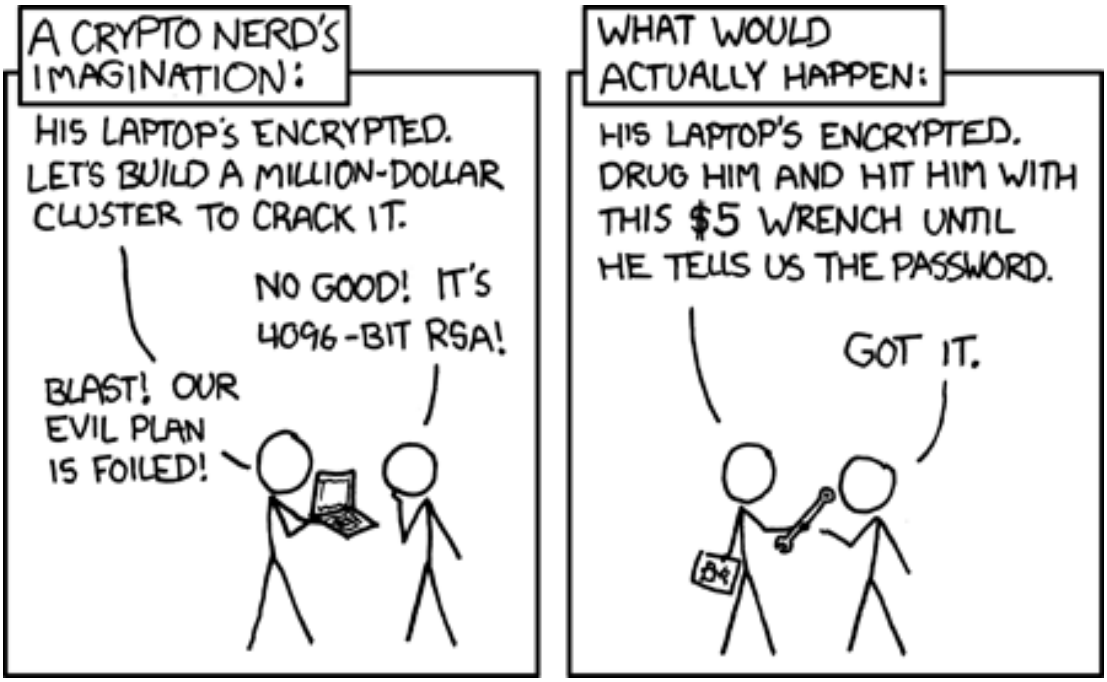
Enabling 2FA wherever you can is still a tremendous enhancement for your account's security, please do it, but remember you can still get pwned while having 2FA, stay vigilant of what accesses you give to third party systems and where you fill your credentials

Lastpass 2FA flaw

Oauth phishing

EvilGinx tool

Top 10 developer crypto mistakes



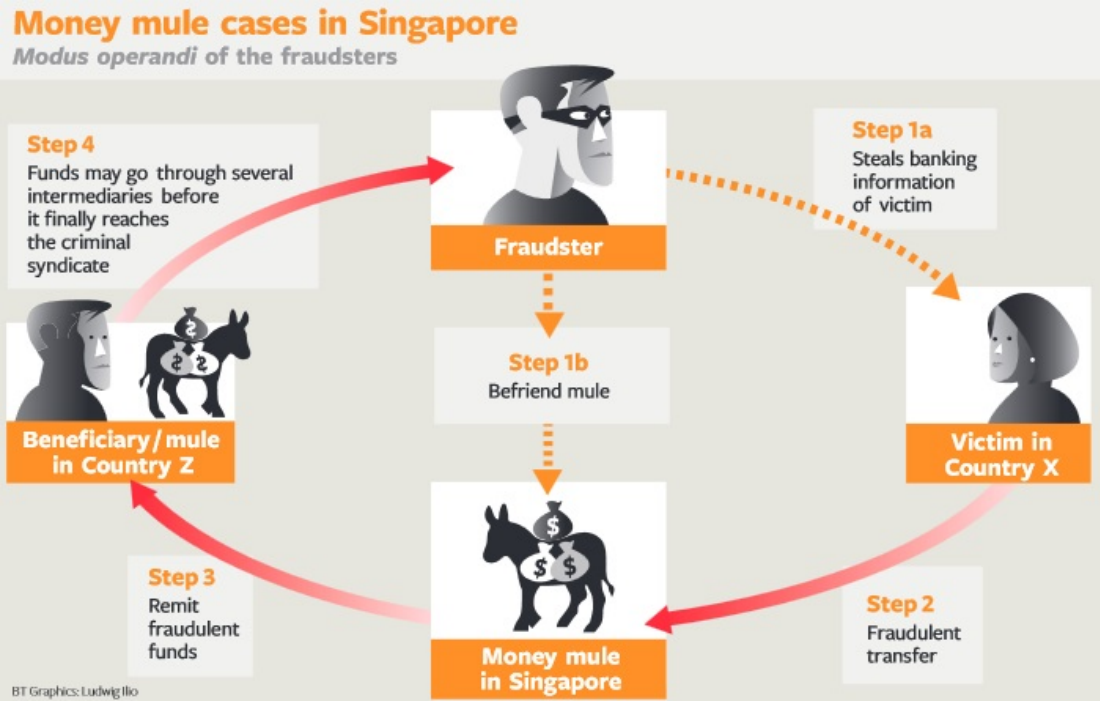
After doing hundreds of security code reviews for companies ranging from small start-ups to large banks and telcos, and after reading hundreds of stack overflow posts on security, the author has composed a list of the top 10 crypto problems I have seen.

Bad crypto is everywhere, unfortunately. The frequency of finding crypto done correctly is much less than the number of times we find it done incorrectly. Many of the problems are due to complex crypto APIs that are insecure by default and have poor documentation. Another reason for so many problems is that finding the issues seems to require manual code analysis by a trained expert. The popular static analysis tools do not do well in finding crypto problems, neither will blackbox penetration tests.

Author's hope in publishing this list is for it to be used by both code reviewers and programmers to improve the state of crypto in software.

Read More

Blind Trust in Email Could Cost You Your Home



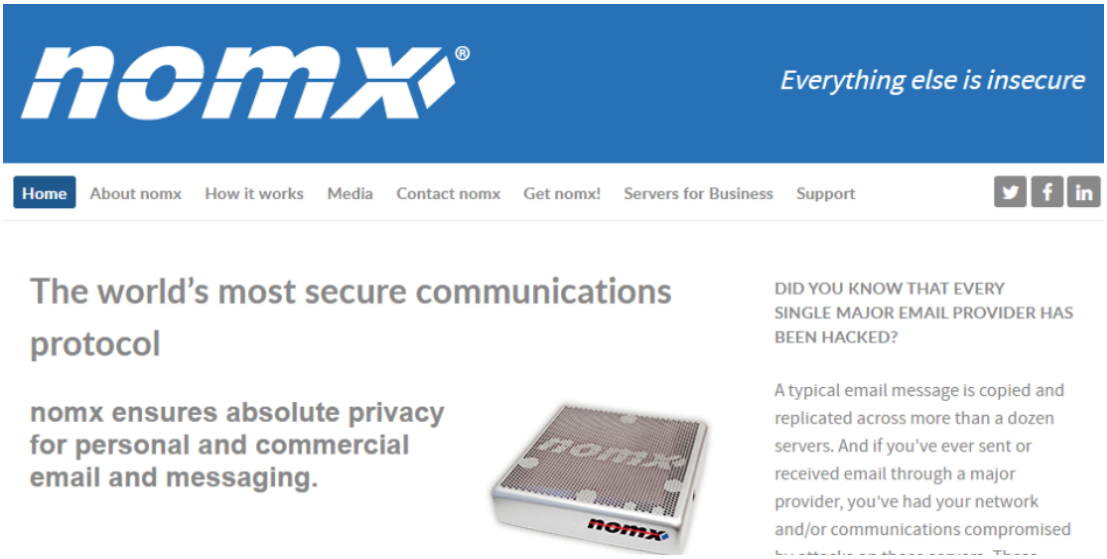
The process of buying or selling a home can be extremely stressful and complex, but imagine the stress that would boil up if — at settlement — your money was wired to scammers in another country instead of to the settlement firm or escrow company. Here's the story about a phishing email that cost a couple their home and left them scrambling for months to recover hundreds of thousands in cash that went missing.

So here's what you need to know if you or anyone you know, love or even like are about to buy or sell a home: Never wire money based on the say-so of one party to the transaction made via email. You simply don't know if their account is hacked, so from a self-preservation standpoint it's best to assume it is.

Always double or even triple check any instructions for wiring money at settlement. Confirm all wiring instructions in person if possible, or else over the phone. By the way, these same precautions can help make organizations less susceptible to CEO fraud schemes, email scams in which the attacker spoofs the boss and tricks an employee at the organization into wiring funds to the fraudster.

Read More

Nomx: The world's most secure communications protocol



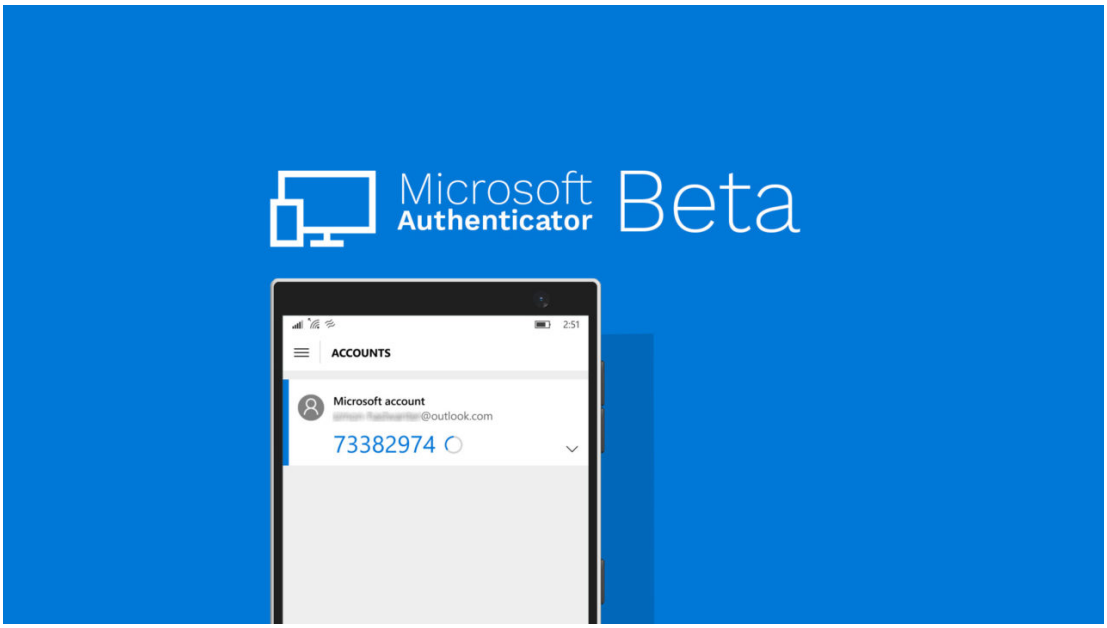
Scott Helme was recently invited to take part in some research by BBC Click, alongside Professor Alan Woodward, to analyse a device that had quite a lot of people all excited. With slick marketing, catchy tag lines and some pretty bold claims about their security, nomx claim to have cracked email security once and for all. Down the rabbit hole we go!

(Spoiler Alert) It would be very easy to conclude that this is a scam. The device is running standard mail server software running on a Raspberry Pi, most of which is outdated. They have presented at countless tech shows and can be constantly found making bold statements of 'absolute security' yet didn't pick up a CSRF vulnerability in their web interface.

This is a case study in need for white hat hackers, responsible disclosure. The BBC Click show dedicated to this investigation will air on 29 April on the BBC News Channel and iPlayer, where it will also be available afterwards.

Read More

Microsoft App Aims to Delete the Password



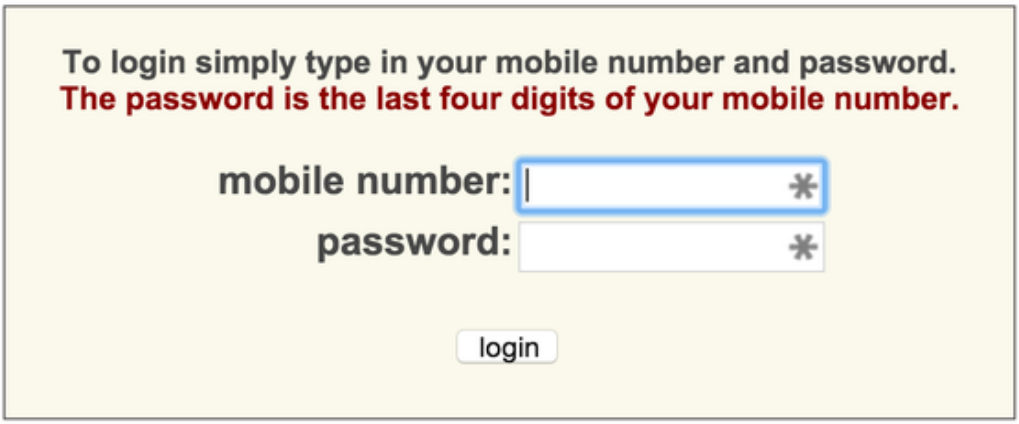
Microsoft took another step toward eliminating passwords with the general availability release of its Authenticator application designed to swap traditional password authentication with push notifications.

After downloading Microsoft Authenticator for iOS or Android devices, you add account information and just enter your username when accessing those websites. Instead of entering a password, you get a push notification. Tap "Approve," and you're logged in.

This isn't Microsoft's first foray into password elimination. Authenticator's implementation model, he says, is similar to that of Windows Hello, which lets users log into Windows 10 devices using biometric authentication.

Read More

Reckon you've seen some stupid security things? Here, hold my beer...



I've seen some very stupid security stuff out there the likes of which make the above example not just believable, but likely. Don't believe me? Here, hold my beer...

Read More

Introducing Cloudflare Orbit: A Private Network for IoT Devices

In October, Cloudflare wrote about a 1.75M rps DDoS attack they mitigated on their network, launched by 52,467 unique IP's, mostly hacked CCTV cameras (Mirai botnet). They continued to see more IoT devices in DDoS attacks, and so they started to put together a security solution to protect the devices from becoming part of the botnet in the first place. Today they're announcing it: Cloudflare Orbit.

Orbit sits one layer before the device and provides a shield of security, so even if the device is running past its operating system's expiration date, Cloudflare protects it from exploits. And while devices may be seldom patched, the Cloudflare security team is shipping code every day, adding new firewall rules to Cloudflare's edge. Think of it like changing IoT to I*oT — devices can still access the Internet, but only after passing through Cloudflare where malicious requests can be filtered.

Instead of writing and shipping a patch, IoT companies can write logic on Cloudflare's edge, and write their own firewall rules to run on Cloudflare, and it updates the Cloudflare Orbit layer immediately, for all of their devices, without their users ever being so much as nudged to install something.

This new feature looks a lot like a cloud-based IDS/Web Application Firewall for IoT. While this is a very good way to have a quick hotfix waiting for the actual patch to be deployed, it is not recommend to rely on this as an alternative to patching, as those filtering can often be bypassed if you put enough effort.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.