From: james | personal genius <[redacted]>
To: [redacted]>
Subject: Fwd: Email Security Recommendations
Date: Fri, 31 Aug 2018 18:49:02 +0000

HI, forwarding to you as an FYI, so you know…

[redacted] suggesting enhanced security for your (and [redacted]) google account(s). If the bosses decide to go this route I'll make sure everything is setup for you and easy to use.

Thank you,

James Ce
your own Personal Genius
□ Certified Support Professional 10.6
http://personalgenius.co

Begin forwarded message:

From: james | personal genius <[redacted]>
Subject: Email Security Recommendations
Date: August 31, 2018 at 2:46:21 PM EDT
To: "jeffrey E." <jeevacation@gmail.com>
Cc: Darren Indyke <[redacted]>, Richard Kahn <[redacted]>

Hello,

I recently had a discussion with another client about email security that I thought would be relevant to you.

Threat Landscape. There are two man risk vectors to emails: the compromise of account credentials through phishing or spear-phishing campaigns and man-in-middle eavesdropping attacks.

Phishing. These attacks attempt to trick people into entering their personal information, passwords and/or credit cards numbers into fake websites. Spear-phishing is the targeted use of phishing attacks to compromise a particular group or organization. *Famously, it was a spear-phishing campaign that allowed the DNC's 2016 emails to be compromised and published online.*

These usually show-up as emails claiming someone has "shared a Google document with you". When you click the link, you're presented with a Google login page that captures the credentials you enter for the attacker. These fraudulent emails have gotten harder to spot and they're now nearly impossible to distinguish from the valid messages.

This problem was so widespread that Google implemented an anti-phishing, mandatory security key policy for all of their employees. They distributed little keychain fobs to exchange super secure secondary keys with your paired devices whenever you need to log into your Google account. Google claims that they haven't had a single confirmed case of accounts being compromised since implementing the policy last year.

Google's Titan Security Keys are now available in U.S for everyone (there's a waiting list). They are $50 each, work with Macs (Chrome) iPhones and iPads. They're compliant with the current & common multi-factor authentication standards, so they work with other applications as well.

I'd recommend we try these keys for Jeffrey, [redacted] and Darren's accounts, and if they prove effective and usable, add them for others that are handling sensitive information. They can be ordered at https://store.google.com/product/titan_security_key_kit

Man-in-the-Middle/Eavesdropping. Email is built on a messaging framework that predates the internet (as we know it) and is inherently insecure. Every email sent (including this one), travels across several privately-owned servers and networks to get to its intended recipients. Messages are always sent as ASCII (plain text) readable to anyone.

The NSA famously has exploited this design flaw by inserting themselves into the companies that run the major internet hubs (such as AT&T) and archiving every email that crosses their networks--which is pretty much all of them. It is safe to assume that other governments' agencies—if not corporate and non-state actors— have implemented similar surveillance systems (Yahoo and AOL were recently exposed to be scanning of their users' messages for ad targeting).

The only way to prevent sensitive information from being exposed to bulk email collection is to encrypt the messages end-to-end, rendering them unreadable to anyone that intercepts them. For regular email host that requires the sender and recipient to exchange cryptographic keys ahead of time, and a difficult (read: almost impossible for regular users) setup process in email programs.

Fortunately, there are several email hosts that specialize in secure email, managing the cryptographic keys for you. You can even send encrypted messages from their services to regular email addresses (the recipient is directed to a webpage where they enter the password you provide them outside of email to decrypt, read and/or reply to your message).

The two best secure hosts are Protonmail ([redacted]) and Hushmail ([redacted]). The both have free or low-cost basic accounts which would be sufficient for limited use (only messages with VERY sensitive information), or professional accounts, to replace whole email presence.

(Neither support the hardware encryption keys discussed above, but they wouldn't be vulnerable to phishing attacks as they don't have linked Google Docs-like services that would prompt you for their passwords.)

If interesting, [redacted] recommend setting up accounts for Darren & Jeffrey to play around with or use as needed for sensitive communications.

Thank you,

James Ce
your own Personal Genius
□ Certified Support Professional 10.6
http://personalgenius.co