From: james | personal genius <[redacted]>
To: Lesley Groff <[redacted]>
Subject: Re: G3 Email Incident Alert
Date: Mon, 25 Sep 2017 20:16:12 +0000
Attachments: IMG_0305.TRIM.MOV

On your phone, please check Settings > Calendar > Default Alert Times and make sure they're all set to None.

And try creating a new test event.

Did you get an email alert for the event I created for 4:25PM?

Thank you,

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

On Jul 27, 2017, at 12:03 PM, Lesley Groff <[redacted]> wrote:

Ok thanks so much James!

Sent from my iPhone

On Jul 26, 2017, at 6:54 PM, james | personal genius <[redacted]> wrote:

So if you log into [redacted] from a new computer, it texts you a code to enter to proceed?

It prevents hackers from accessing your account/email/google drive without your knowledge -- even if they managed to get your password. It can be a pain in the arse to have to do the extra step all the time.

I ask because if I were a nefarious hacker trying to spy on JEE, your account would be what I would target — rich store of data attached to someone that fields unexpected contact requests constantly so much easier to "social engineer".

Thank you,

James Ce, your Personal Genius,
http://personalgenius.us

On Jul 26, 2017, at 5:32 PM, Lesley Groff <[redacted]> wrote:

I do on my cell phone I believe…

On Jul 26, 2017, at 5:24 PM, james | personal genius <[redacted]> wrote:

Do you have 2 factor authentication turned on for your Google Account? I don't recall if we've discussed this in the past, but it might be a good idea.

James Ce, your Personal Genius,
http://personalgenius.us

On Jul 26, 2017, at 5:09 PM, Lesley Groff <[redacted]> wrote:

Ok. Thank goodness. I almost got scared after opening this email!

Sent from my iPhone

On Jul 26, 2017, at 5:00 PM, james | personal genius <[redacted]> wrote:

Thanks for the heads up. As long as you didn't try to log into the fake site, we're safe. 🙃

James Ce, your Personal Genius,
http://personalgenius.us

On Jul 26, 2017, at 4:57 PM, Lesley Groff <[redacted]> wrote:

I did receive the email they are discussing yesterday. I did not open it and deleted right away. I figured it was something bad. Wanted you to see this though.

Sent from my iPhone

Begin forwarded message:

From: Marco Merida, G3 Global Services, LLC <[redacted]>
Date: July 26, 2017 at 2:28:42 PM EDT
To: <[redacted]>
Subject: G3 Email Incident Alert
Reply-To: Marco Merida, G3 Global Services, LLC <[redacted]>

Good afternoon.

This is to inform that you received an email from [redacted] with the subject line "25/07/17" on, or after 4:40pm yesterday and it should NOT be opened. As a further precaution, you should notify your IT department as they will likely require additional measures per your organization's IT protocols, such as deleting the email and deleting it from the deleted items folder.

In summary, a single G3 user's email address book was compromised in Office 365 using Outlook Web Access. The intrusion was detected promptly, and the account was disabled in less than one hour. All emails and attachments sent were scanned by 30 different antivirus vendors to identify malicious content. We determined there is a malicious link in the attachment.

If followed, this link will take a user to a phishing site to obtain a username and password. Internet Explorer Smart Screen will alert a user that opens the attachment (and click the link) that they should not proceed, however you should actively be advising any recipients of this message to not open the email or attachment and coordinate with your IT team.

To emphasize, based on our internal IT security measures and protocols, NO CUSTOMER DATA was compromised, with the exception of email addresses. Upon detection, we immediately conducted leadership meetings and engaged a third-party IT consulting firm to control, assess, monitor, and advise on the situation. However, in spite of these measures, the infected attachment was sent.

As a result, we are deploying the following measures:

1. Immediate password reset with even more stringent password controls

2. Mandate of auxiliary company-wide security training

3. Conducting client communications to advise of the email concern

We at G3 Global Services hold our clients' information with the utmost importance. We felt compelled to inform you of the situation and advise that while no private information was compromised through this isolated event, a malicious link was detected and your firm should engage its IT security protocols to protect against further issues.

We sincerely apologize for this inconvenience.

If you have any questions, please feel free to connect with Janet Vrasic, Director of Customer Relationships or myself as our Chief Strategy Officer per the contact information below.

Contact:
Janet Vrasic
312.948.0413
[redacted]

Thank you,
Marco A. Merida
Chief Strategy Officer

G3 Global Services, LLC
201 S. Narcissus Ave., Suite 2
West Palm Beach, FL 33401
tel: [redacted]

[redacted]
[redacted]
u=210269d36b1b3382d74f9d40f&id=572a935334&e=51920f7d36

==========
==========

Unsubscribe [redacted] from this list:
[redacted]
u=210269d36b1b3382d74f9d40f&id=3bd9bbf3a5&e=51920f7d36&c=db399d9ca9