Keystone
TECHNOLOGY CONSULTANTS

Cybersecurity Tips and Reminders

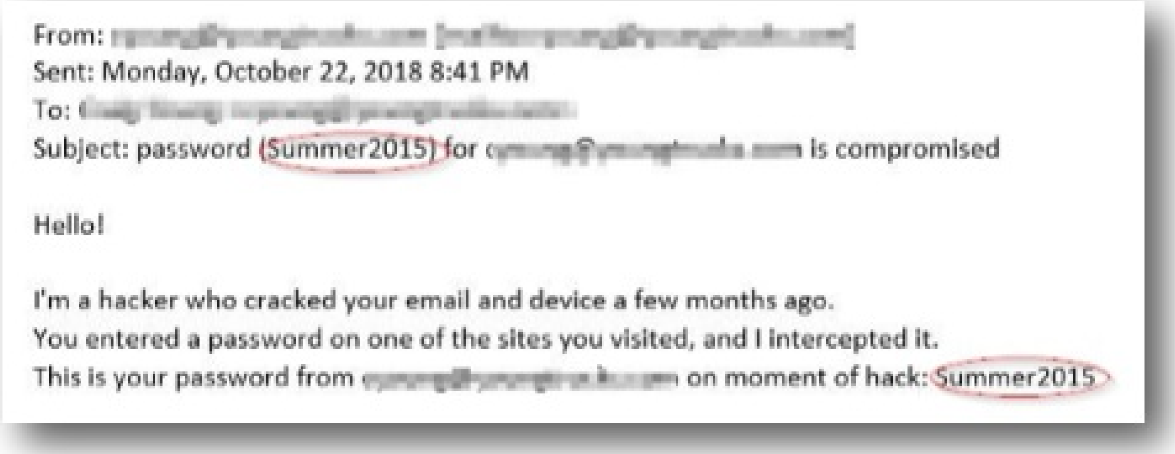
This Month's Focus- Your Account Has Been Hacked?

Below is a screenshot of a spam message that has been making the rounds lately. It is especially alarming to recipients because it is made to appear like it was sent from the user’s email account AND the password that is referenced is one that was used somewhere in the past by the owner of the email account. The spam message goes on to say they have incriminating information about the person and that they will release all this information, as well as compromising photos, to everyone in this person’s email contact list…..IF they do not pay the Bitcoin ransom within 48 hours. On the surface, all this can be very concerning to a recipient because much of it appears real to them….ESPECIALLY the familiar password.

Send me more info

Be Suspicious. Something is not Right.

Fortunately, their email account and their computer systems have not been hacked like the spammer wants them to believe. Unfortunately, a website or several websites they have created accounts on have been hacked in the past. If you follow information technology news groups, you will read about customer data breaches (hacks) on a weekly basis. The most widely known breach was the Equifax breach reported September 2017 where 148 million people had their personal credit information compromised and sold on the black market. Hackers get to these databases by illegally gaining access to the backend infrastructure of websites. Typically, the customer information hacked is name, email address, and password used for the website. When hackers gain access to this information they download it and then sell it on the black market for creative hackers to exploit in many different ways. The hacker in the above spam message got this name, email address, and password from a customer database breach.



From: [redacted]
Sent: Monday, October 22, 2018 8:41 PM
To: [redacted]
Subject: password (Summer2015) for [redacted] is compromised

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from [redacted] on moment of hack: Summer2015

There is a great website, haveibeenpwned.com , where you can enter your email address to see if it has been part of any of the know customer database breaches. You may find that your address has been part of one or many breaches. What do you do then? Look at the date of the breach and ask yourself if you have changed passwords associated with that email address since the breach report date….if you haven’t, change it ASAP! If you have, you are likely safe.

All this really goes back to having good password habits.

1. Avoid using the same password across many platforms. Hackers will try to go to common sites and try credentials they have bought to see if they work elsewhere.
2. Change passwords frequently to avoid the risk of a hacker using an old password that still may be valid.
3. Use long passwords that will be harder for automated hacking systems to hack.

You may ask yourself, how do I remember all these long, unique passwords that I am always changing? We suggest using a password manager like LastPass to help you create, save, and even enter passwords. It will help keep your online life that much safer.

Any Questions?

Please respond to this email if you have questions, comments, or desire more information.

Keystone Technology Consultants| Keystonecorp.com