

# Case Study: Hacking the Hackers

Demonstrating how cyber criminals easily target and breach small businesses.



[www.csid.com](http://www.csid.com)

# SUMMARY

---

With [30% of spear-phishing attacks targeted at businesses with fewer than 250 employees](#), small and medium-sized businesses are a major target for cyber criminals looking to steal identities and credit card information with high spending limits. Despite this growing threat, most small businesses (SMBs) are not taking proactive measures to protect against cyber criminals. In fact, [for every 10 SMBs](#), at least 3 are not taking any measures to protect their business against security threats, leaving private data exposed to cyber criminal activity. With [the median fraud loss for a small to medium-sized business coming in at about \\$200,000](#), many SMBs that are breached have no other option but to close up shop. And disturbingly, only 12% of SMBs actually have a breach preparedness plan in place.

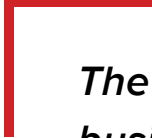
To demonstrate just how effortlessly cyber criminals are targeting and exploiting SMBs, CSID reinforced the need for data breach mitigation by executing an experiment. The idea? Develop a mock business, build its presence online and watch as it becomes a target for real cyber criminals to hack.

And thus, Jomoco was born, a fictitious coconut water company with two fabricated employees, Rachel and Richard. CSID established the virtual presence of Jomoco in a similar way a start-up would: buy a URL, set up a web server and create employee business email addresses. The team developed additional personal profiles for the Jomoco's two employees – an Xbox Live account for Rachel, a Facebook account for Richard, and personal emails for both – to mimic the cyber footprints that might exist for real small business owners.

## MATERIALS WE USED

- Jomoco business URL
- Jomoco website server
- Jomoco business credit card
- Jomoco business email accounts for employees Rachel and Richard
- Personal email accounts for employees Rachel and Richard
- Personal Xbox Live account with \$15 credit (tied to a personal credit card) for employee Rachel
- Personal Facebook account for employee Richard

To see how quickly Jomoco would be breached, CSID set up online accounts associated with the company and its employees without taking extra steps to ensure security. Furthermore, CSID ensured that Jomoco's fictional employees made common mistakes when it came to protecting their professional and personal data online. The real cyber criminals took it from there.



***The idea? Develop a mock business, build its presence online and watch as it becomes a target for real cyber criminals to hack.***

# WHAT HAPPENED

---

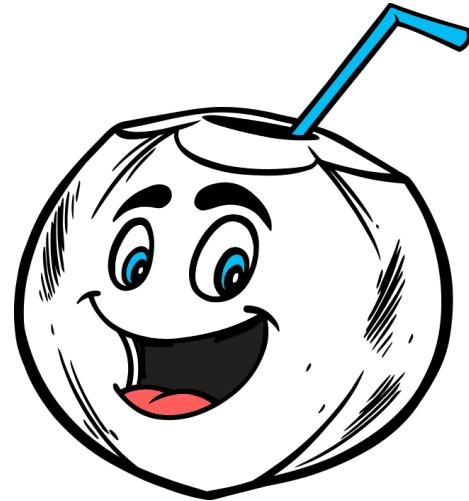
In just 30 minutes, employees' personal accounts were locked out. Within an hour, the Jomoco server was down, the website defaced and the business credit card fraudulently used. How did this happen? Let's follow the path real cyber criminals took to exploit Jomoco and its employees.

First, the hackers accessed Rachel's personal email address by easily cracking her poor password. Since the fictional Rachel made the mistake of reusing passwords across multiple accounts – something [61% of consumers do in real life](#) – cyber criminals were also able to hack into her Xbox Live account and lock her out using the same credentials. In doing so, they stole both her Xbox gaming identity and the \$15 Xbox Live credit attached to it, information and currency that has nothing to do with Jomoco.

It was easy for hackers to access Rachel's business email account using the credentials they had already tried. There, they found a fabricated email to Richard sharing Jomoco's web server details like IP address and login credentials. Using this information, hackers defaced the Jomoco website and locked out the business email accounts and web server, seemingly for fun. Since Richard reused passwords across his personal and professional online accounts as well, the hackers were now also able to access his personal email account and Facebook, where they changed the passwords to both accounts and took them over.

Furthermore, the company credit card was fraudulently used for real purchases. On a positive note, the bank hosting the company credit card froze the account almost immediately after the first fraudulent purchases were made. Using monitoring solutions, the bank identified the fraudulent credit card activity and shut down the account before additional purchases could be made.

Within one hour of Jomoco's cyber footprint emerging online, the cyber presence of the company and its employees was completely compromised.



***"Jomoco is the only coconut water company that uses juice from young Bolivian coconuts cryogenically frozen for over 100 years."***

This exercise demonstrated how easily and quickly cyber criminals can infiltrate the cyber identities of SMBs and the employees associated with them. Rachel's and Richard's password reuse across multiple online accounts – a common mistake representative of the poor password security habits many employees use in real life – was the key to Jomoco's downfall. After cyber criminals hacked only one set of credentials, a chain reaction had begun, enabling access to additional online accounts and valuable, private information. Rachel and Richard also shared sensitive information with one another over email. Sharing secure details, such as login information, Social Security numbers and financial information is extremely insecure and can expose sensitive information to cyber criminals if an email account is breached.

*Hackers locked Rachel out of her Xbox Live account by changing her password. Since she reused her password on multiple sites, they were able to access her gmail account by trying the same credentials. They also stole her \$15 Xbox Live credit and her gaming identity.*



Sign in with your Microsoft account email and password.

That password is incorrect. Be sure you're using the password for your Microsoft account.

Microsoft account [What's this?](#)

☐ Keep me signed in

[Sign in](#)

*This is a fabricated email between Jomoco employees sharing server credentials. Cyber criminals used this information to shut down the Jomoco server and deface the website.*

**Richard**

To: rachel

Cc: richard@jomoco.rocks

Re: Server Settings

9 March 2015 01:09

[Hide Details](#)

1

Thanks Rachel. Getting ready to get things going on our end! All very very exciting. Looking forwards to seeing the new office space. I'll get the web dev guys to login and start work on the page now. Thanks again!!!

Rich

[See More from rachel](#)

**rachel**

To: richard@jomoco.rocks

Server Settings

9 March 2015 01:07

[Hide Details](#)

Inbox - richard@jomoco.rocks

Hey Richard,  
Server is all setup and working. Hope you should know that though by receiving this email :) !  
James asked me to forward across the server settings so you can get the web guys to configure the new landing page.  
Cant wait to go loco for jomoco..... so excited!!

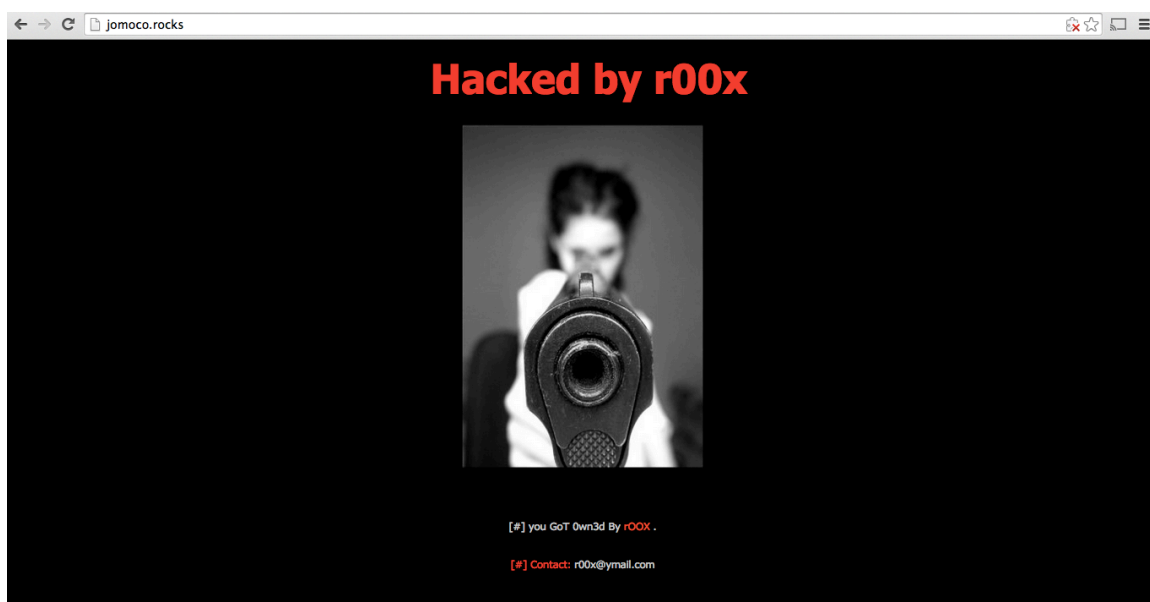
ip: 173.255.139.242

root pass: ErrSwZ5tL3jL

Lots of love,

Rachel x

Jomoco's website, Jomoco.rocks, was defaced by a hacker. Just as a graffiti artist has a signature "tag," so does a hacker. This image is a "tag" or symbol of the hacker r00x.



Jomoco's credit card number was shared in an Internet Relay Chat (IRC) room. A cyber criminal used the credit card to make fraudulent purchases, but the card was flagged by the bank hosting the card through its monitoring services.

```
ckowaej329 Ichk [redacted]
gux lbank [redacted]
CrimeBANK BANK:;VISA;CHASE BANK USA N.A.;CREDIT;SIGNATURE;UNITED STATES;US;USA;;WWW.CHASE.COM;1-800-432-3117 OR
1-302-594-8200
* LimitServ sets channel limit to 529
jameia6 you might me so lonely
berburik ckowaej329 : - $9.53 : DECLINED! - Decline - BANK : VISA - CHASE BANK USA, N.A. -
CREDIT - SIGNATURE - UNITED STATES - Credit : 220
438857 : VISA - CHASE BANK USA, N.A. - CREDIT - SIGNATURE - UNITED STATES -
Ichk 4718492541315119 0723 102
lbank 471849
berburik BANK:;VISA;TARGET BANK;DEBIT;PREPAID;UNITED STATES;US;USA;;
jajb : - $5.24 : APPROVED!! - BANK : VISA - TARGET BANK - DEBIT - PREPAID - UNITED
STATES - REDCARD.TARGET - 1.888.729.7331 Credit : 219
471849 : VISA - TARGET BANK - DEBIT - PREPAID - UNITED STATES - REDCARD.TARGET - 1.888.729.7331
* latitude (latitude[redacted].IP) has joined #unix
MAVxz
* dirbg [redacted] Billings|Montana|59105|United States|
* dirbg [redacted] Billings|Montana|59105|United States|
* LimitServ sets channel limit to 530
MAVxz : - $6.25 : DECLINED! - Decline - BANK : Unknown Credit : 218
ckowaej329 Ichk [redacted]
* Luick (~androlrc@C6BAE039.5CB442D8.365B2C0E.IP) has joined #unix
luckbo30 dec
gux lbank [redacted]
CrimeBANK BANK:;VISA;PFA CARD SERVICES N.A.;CREDIT;SIGNATURE;UNITED STATES;US;USA;;1.800.932.6262
berburik * LimitServ sets channel limit to 531
ckowaej329 : - $1.85 : DECLINED! - Decline - BANK : VISA - BANK OF AMERICA - CREDIT
- SIGNATURE - UNITED STATES - Credit : 217
berburik : VISA - BANK OF AMERICA - CREDIT - SIGNATURE - UNITED STATES -
Trichko Ichk [redacted]
jajb [redacted] Austin|Texas|78759|United States|
gux lbank [redacted]
CrimeBANK BANK:;AMERICAN EXPRESS;AMERICAN EXPRESS COMPANY;CREDIT;UNITED STATES;US;USA;;WWW.AMERICANEXPRESS.COM;
1-800-528-4800
* karbonik has quit (Ping timeout: 180 seconds)
berburik Trichko : - $5.58 : APPROVED!! - BANK : AMERICAN EXPRESS - COMPANY - CREDIT - UNITED
STATES - Credit : 216
berburik 372587 : AMERICAN EXPRESS - COMPANY - CREDIT - UNITED STATES -
```

*To recap, here's a chronological timeframe of everything that happened.*

<b>PERSONAL EMAIL ACCOUNTS</b>	<b>LOCKED OUT WITHIN 15 MINUTES</b>
<b>PERSONAL XBOX ACCOUNT</b>	<b>LOCKED OUT WITHIN 30 MINUTES</b>
<b>PERSONAL CREDIT CARD</b>	<b>DEFRAUDED WITHIN 30 MINUTES</b>
<b>PERSONAL FACEBOOK ACCOUNT</b>	<b>LOCKED OUT WITHIN 30 MINUTES</b>
<b>BUSINESS EMAIL SERVER</b>	<b>HACKED WITHIN 1 HOUR</b>
<b>BUSINESS WEB PAGE</b>	<b>DEFACED WITHIN 1 HOUR</b>
<b>BUSINESS SERVER</b>	<b>LOCKED OUT WITHIN 1 HOUR</b>
<b>BUSINESS CREDIT CARD</b>	<b>DEFRAUDED WITHIN 1 HOUR</b>

# CONCLUSION

---

In less than an hour, Jomoco's fledgling coconut water business was brought to a halt by enterprising hackers. This quickness and ease of the breach underscores how critical it is for SMBs to make cyber security a priority. Understanding and educating employees about the security risks associated with establishing and running a small and medium sized business is the first step in mitigating risk. Here are additional ways SMBs can prevent cyber criminals from exploiting their business:

## DEVELOP SECURITY POLICIES EARLY AND EDUCATE EMPLOYEES

Ensure employees understand the importance of workplace cybersecurity. Create and enforce password, BYOD and social media policies from day one. Encrypt valuable data from employees, customers and partners, like email addresses, passwords and credit card numbers. Require that employees use a VPN when on wireless Internet and regularly update devices. The more well educated the workforce is on the importance of security, the more likely they will be to employ better online habits at work and at home.

## MONITOR EMPLOYEE AND CUSTOMER CREDENTIALS AND YOUR BUSINESS CREDIT SCORE

Take advantage of software solutions that can help monitor the security of your business. A monitoring service can keep track of your SMB's overall health and mitigate the risk of breach. Monitor employee and customer credentials and business credit score to detect fraudulent activity early.

## CREATE A BREACH PREPAREDNESS PLAN

Have a breach preparedness plan in place. Practice transparent communication with the public and affected parties. Hiding details about a breach breeds distrust with customers, which can affect your business reputation. While a damage control plan may not reduce the cost of repairing the breach, it can keep customer relationships in tact and diminish reputation damage.

# ABOUT CSID

---

CSID is the leading provider of global identity protection and fraud detection technologies and solutions for businesses, their employees, and consumers. With CSID's advanced enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection products advance from credit monitoring to include a full suite of identity monitoring services; insurance and full-service restoration; and proactive breach mitigation and resolution.

[www.csid.com](http://www.csid.com)