



# Vulnerability Disclosure in IoT: The good, the bad and the legal threats

Mark Neve, Copper Horse  
@copperhorseuk

IoT Security Foundation Annual Conference  
26<sup>th</sup> November 2019

# Vulnerability Disclosure – Introduction

“Many well-intentioned people simply give up and don’t report serious security incidents when the effort is too high or the risk is too great” — security expert Troy Hunt



## Code of Practice for Consumer IoT Security

### 2) Implement a vulnerability disclosure policy

All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.



<https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security>

# Who's Testing Your Security?

**Why Do You Hack?**



<https://www.hackerone.com/sites/default/files>

**Why Do You Choose  
The Companies You Hack?**

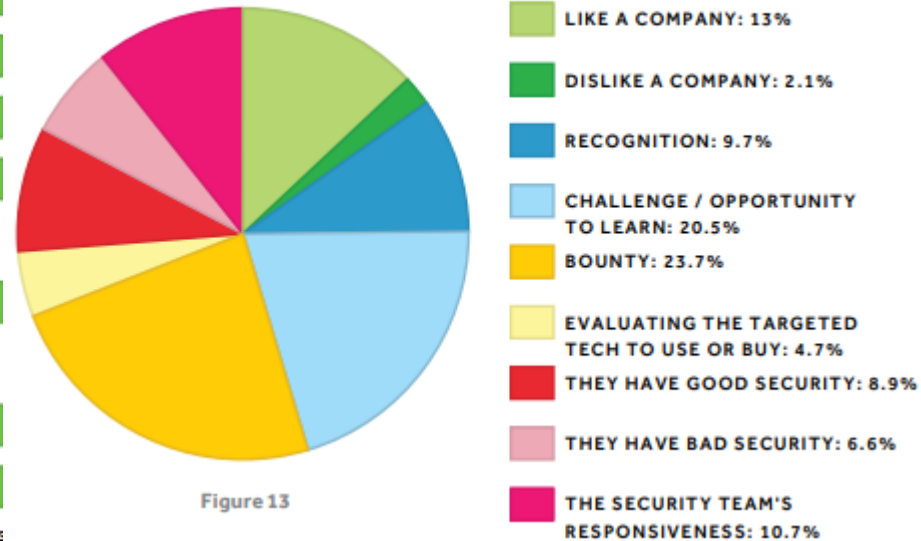


Figure 13

- Other bad reasons, not always discovered through disclosure!



# Best Practice

- Coordinated Vulnerability Disclosure
- Define your disclosure policy
- What's “acceptable” testing?
- Specify your disclosure timeline – usually 90 days
- Nominate a Head of Security Response



# Vulnerability Disclosure: Best Practice 2/2

- <companydomain>/security page
- Thank you page
- Setup contact email addresses:
  - security@<companydomain> and securityalert@<companydomain>
- PGP key



# Proxy Disclosure

## Bug Bounty Payouts Up 73% Per Vulnerability: Bugcrowd

Bug bounty programs grew along with payouts, which averaged \$781 per vulnerability this year, researchers report.

## WHAT IS HACKER101?

Hacker101 is a collection of videos, resources, and hands-on activities that will teach you everything you need to operate as a bug bounty hunter. The material is available to learn for free from HackerOne. Led by HackerOne's Cody Brocious, the Hacker101 material is ideal for beginners through to intermediate hackers and located at <https://hacker101.com/>. Feel free to share and join the conversation on Twitter with hashtag #hacker101.

## Bugcrowd University Expands Education and Training for Whitehat Hackers

## Bugcrowd Pays Out Over \$500K in Bounties in One Week

In all, bug hunters from around the world submitted over 6,500 vulnerabilities in October alone.

[https://www.darkreading.com/vulnerabilities---threats/bugcrowd-pays-out-over-\\$500k-in-bounties-in-one-week/d/d-id/1336307](https://www.darkreading.com/vulnerabilities---threats/bugcrowd-pays-out-over-$500k-in-bounties-in-one-week/d/d-id/1336307)



# Zero-Day Market

## We are Zerodium

The leading exploit acquisition platform for premium zero-days and advanced cybersecurity capabilities.

"We pay BIG bounties, not bug bounties"

### ZERODIUM Payouts for Mobiles\*

FCP: Full Chain with Persistence  
RCE: Remote Code Execution  
LPE: Local Privilege Escalation  
SBX: Sandbox Escape or Bypass

■ iOS  
■ Android  
■ Any OS

ZERODIUM Payouts for Mobiles\*

Up to \$2,500,000

Up to \$2,000,000

Up to \$1,500,000

Up to \$1,000,000

Up to \$500,000

Up to \$200,000

Up to \$100,000

FCP: Full Chain with Persistence  
RCE: Remote Code Execution  
LPE: Local Privilege Escalation  
SBX: Sandbox Escape or Bypass

iOS

Android

Any OS

1.001

Android FCP  
Zero Click

Android

1.002

iOS FCP  
Zero Click

iOS

2.001

WhatsApp  
RCE+LPE  
Zero Click

iOS/Android

2.002

iMessage  
RCE+LPE  
Zero Click

iOS

2.003

WhatsApp  
RCE+LPE

iOS/Android

2.004

SMS/MMS  
RCE+LPE

iOS/Android

3.001

Persistence

iOS

2.005

WeChat  
RCE+LPE

iOS/Android

2.006

iMessage  
RCE+LPE

iOS

2.007

FB Messenger  
RCE+LPE

iOS/Android

2.008

Signal  
RCE+LPE

iOS/Android

2.009

Telegram  
RCE+LPE

iOS/Android

2.010

Email App  
RCE+LPE

iOS/Android

4.001

Chrome  
RCE+LPE

Android

4.002

Safari  
RCE+LPE

iOS

5.001

Baseband  
RCE+LPE

iOS/Android

6.001

LPE to  
Kernel/Root

iOS/Android

2.011

Media Files  
RCE+LPE

iOS/Android

2.012

Documents  
RCE+LPE

iOS/Android

4.003

SBX  
for Chrome

Android

4.004

Chrome RCE  
w/o SBX

Android

4.005

SBX  
for Safari

iOS

4.006

Safari RCE  
w/o SBX

iOS

7.001

Code Signing  
Bypass

iOS/Android

5.002

WiFi  
RCE

iOS/Android

5.003

RCE  
via MiTM

iOS/Android

8.002

LPE to  
System

Android

8.001

Information  
Disclosure

iOS/Android

8.002

[k]ASLR  
Bypass

iOS/Android

9.001

PIN  
Bypass

Android

9.002

Passcode  
Bypass

iOS

9.003

Touch ID  
Bypass

iOS

\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com



# The Legal Threats

## York council app users hacked: Nearly 6,000 affected

20 November 2018



Screenshot of the Council's justification for reporting our developer to the police

## One Planet York: 'Ethical hacker' exposed council app flaw

28 November 2018



Follow

@troyhunt @Scott\_Helme We are aware of the York 'data breach' but please be reassured we don't regard this incident as criminal. We recognise the benefits of software vuln disclosure as part of a healthy security environment and the researcher has acted correctly.

11:10 AM - 26 Nov 2018

90 Retweets 455 Likes

29 90

On Monday, the council tweeted: "Despite attempts to contact [the hacker], they did not respond and as a result of what appears to be a deliberate and unauthorised access we informed the police".

Screenshot of

### More stories from around Yorkshire

The local authority, which has since revised its stance, said: "Following further review it has become clear that the person who identified the issue with the app had tried to contact us but their email had not been received due to security settings.

<https://www.rapidspike.com/blog/one-planet-york-data-breach-update/>





# Passing the Responsibility

## Five million customers affected by Vtech database hack

By Zoe Kleinman  
Technology reporter, BBC News

30 November 2015

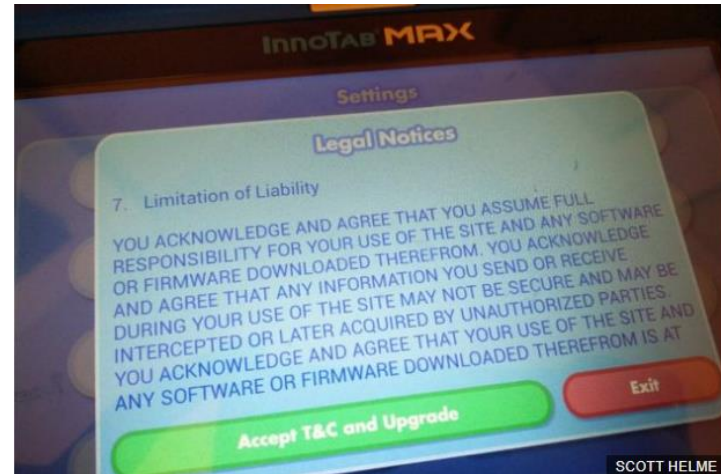


The hacked database included a lot of customer data, including some details about children, and the company was told about the breach by a journalist.

It did not contain any credit card information, Vtech said, but it did store the "name, email address, encrypted password, secret question and answer for password retrieval, IP address, mailing address and download history" of customers.

## VTech issues new T&Cs telling parents to take responsibility if children's tablets and toys get hacked

VTech was hacked in December leading to breach of personal data and 'pictures of kids'



<https://www.bbc.co.uk/news/technology-35532644>

<https://www.independent.co.uk/news/uk/home-news/vtech-issues-new-terms-and-conditions-telling-parents-to-take-responsibility-if-childrens-tablets-a6865331.html>



# Doing it Right

- Keep a timeline
- Be nice
- Proof of concept
- Communicate
- Deploy fixes
- Joint disclosure
- Say thanks
- Security Advisory



## Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies



# 2018 vs 2019 Research Data



# Thanks!

@copperhorseuk

[mark.neve@copperhorse.co.uk](mailto:mark.neve@copperhorse.co.uk)

