FIVE STEPS TO DEFEND AGAINST SOCIAL MEDIA WEAPONIZATION

Nick Hayes
Senior Analyst, Forrester Research
@nickhayes10
The ORGANIZATION sought, in part, to conduct what it called “information warfare against the United States of America” through fictitious U.S. personas on social media platforms and other Internet-based media.

By in or around May 2014, the ORGANIZATION’s strategy included interfering with the 2016 U.S. presidential election, with the stated goal of “spread[ing] distrust towards the candidates and the political system in general.”
Less and less control of your attack surface

- Nefarious threats, mentions, and sales on unaffiliated channels
- Fraudulent or malicious spoofing and impersonations
- Unsanctioned, rogue activity and occurrences of affiliated footprint
- Known, corporate-controlled digital footprint
So many ways to make mistakes – and attackers only need one

Employees post PII

SOC analysts leak contact info

VIPs & execs risk physical safety
Tactics can be sophisticated
They’re effective too
Fake accounts are easy to come by
Timothy Stokes
Recruitment Consultant at Teledyne Technologies Incorporated
Newbury Park, California | Electrical/Electronic Manufacturing

Current
Teledyne Technologies Incorporated
Previous
ExxonMobil
Education
University of California, San Diego

500+ connections

Summary
I assist in selecting the best-qualified candidates during open hiring. I am involved with screening applications, interviewing candidates and checking references. Our contracts involve the recruitment and secondment of skilled engineers, technicians and managers to client facilities on a domestic or international basis to support major engineering, construction, installation and ongoing operations activities. Teledyne Technologies Inc. owns a globally focused operation, active in over 40 locations, driven by a professional and talented team of people, dedicated to achieving excellence.

Experience
Recruitment Consultant
Teledyne Technologies Incorporated
March 2012 – Present (3 years 5 months) | Thousand Oaks

- Remarkable experience in Recruitment Consultancy
- Project based recruitment, candidate screening & referral networking for both local and emerging
- Ability to identify and successfully qualify candidates
- Familiarity with payroll procedures and taxation issues relevant to contractors
- Good understanding of Consultants contracts and terms and conditions
- Amazing ability to manage independently

Hundreds of connections enhance the account’s credibility.

Photos of real people, along with common names and plausible job experience and office locations, make the accounts appear legitimate.

Job summaries are well-written and often copied or mimicked from other real profiles.

Fake accounts frequently pose as recruiters on LinkedIn to entice more users to connect.
#RSAC

Fake accounts and why you should care
FB’S MONTHLY AVERAGE USERS (MAUs) AND FAKE ACCOUNTS

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg monthly active users</td>
<td>1,517</td>
<td>1,754</td>
<td>2,036</td>
</tr>
<tr>
<td>Avg ann revenue, per user</td>
<td>$11.69</td>
<td>$15.98</td>
<td>$20.21</td>
</tr>
<tr>
<td>Avg monthly “false” accts</td>
<td>106m (7%)</td>
<td>123m (7%)</td>
<td>285m (14%)</td>
</tr>
<tr>
<td>Duplicate</td>
<td>76m (5%)</td>
<td>105m (6%)</td>
<td>204m (10%)</td>
</tr>
<tr>
<td>Undesirable</td>
<td>30m (2%)</td>
<td>18m (1%)</td>
<td>81m (4%)</td>
</tr>
<tr>
<td>Wasted marketing spend (in $US millions)</td>
<td>$1,241</td>
<td>$1,962</td>
<td>$5,761</td>
</tr>
</tbody>
</table>

Forrester
A far bigger problem than ANY social network will admit

- Estimates on rolling basis (i.e., inclusive of security efforts).
- Does NOT discuss false accounts as they pertain to:
  - Instagram, WhatsApp, or Oculus.
- Calculations based on what social networks are *aware of*:
  - Twitter states approx. 5% of its MAUs are spam accounts.
  - LinkedIn claimed it didn’t have an accurate way to count fake accts!
  - Possible that far more go undetected.
Existing mitigation methods are inefficient (at best).
You need active visibility to protect your externally-facing digital footprint.
Turn digital risk insight into risk action.
“Mean time to remediation” is a crucial KPI

Best opportunity to realize efficiencies
Five core actions of digital risk protection

- Onboard
- Link
- Identify
- Enforce
- Resolve
Simplify further to three key steps

**Map**
- **Onboard** business attributes, actors and assets to chart digital footprint.
- **Link** digital assets to business attributes, actors, and IP.

**Monitor**
- **Identify** and analyze risk events based on *business relevance* and *risk severity*, including indicators of attack, compromise, and abuse.

**Mitigate**
- **Enforce** controls via technical integration w/ digital assets & infrastructure.
- **Resolve** events via takedown requests, patching, IP blacklisting, cease and desists, law enforcement coordination, and other response options.
Map business context for better risk scoring
Actively monitor your digital assets at risk.
Prepare your digital extortion decision tree to mitigate impact.
Address capability gaps

<table>
<thead>
<tr>
<th>Channel type</th>
<th>Map</th>
<th>Monitor</th>
<th>Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social</td>
<td>◯</td>
<td>●</td>
<td>◯</td>
</tr>
<tr>
<td>Mobile</td>
<td>◯</td>
<td>◯</td>
<td>○</td>
</tr>
<tr>
<td>Web</td>
<td>◯</td>
<td>◯</td>
<td>◯</td>
</tr>
<tr>
<td>Dark web</td>
<td>◯</td>
<td>◯</td>
<td>○</td>
</tr>
</tbody>
</table>

Less mature ○ > More mature ●
Digital distortion is just beginning.
Final recommendations

1. Start small, tackle 1-3 use-cases at first.

2. Recalculate your digital risk exposure to strengthen your ROI.

3. Prioritize action – onboarding, takedowns, response, etc.
THANK YOU

Nick Hayes
@nickhayes10