

[Having trouble viewing this message? Please click here.](#)

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks



CYBERSECURITY

[FIN8 Back in Business Stealing Credit Card Information with Badhatch](#)

Security research firm Gigamon has reported that the nasty cybercriminal group FIN8 may have reappeared in June after a two-year silence. FIN8 is known for implementing malware on point of sale systems to steal credit card information and selling it on the dark web.

FIN8 appears to be back in business with a new twist on its old scheme. [Read more](#)

DATA SECURITY

[Phishing Attacks Target Office365 Administrators](#)

As reported on July 24 by [Help Net Security](#), hackers are targeting Microsoft Office365 administrators in a new phishing campaign that can obtain and confirm credentials in real time. According to the article, the attack begins with a fake Office365 notification where all the links in the message link back to fake Office365 sites at the windows.net domain. A script on the fake site checks the validity of the administrator's credentials in real time via an IMAP connection back to the real Office365 portal. If the credentials authenticate successfully, the attackers download the entirety of the administrator's mailbox via the IMAP connection completely undenounced to the administrator. Finally, the administrator is redirected to their actual MS Office365 Exchange Online mailbox. [Read more](#)

DATA BREACH

[Health Care Organizations Have Highest Costs for Data Breaches](#)

As readers of this blog know, data breaches in the health care industry are all too common. Health care organizations are an attractive target for hackers because of the nature and amount of personal information that they possess.

Therefore, it is perhaps not surprising that health care organizations have the highest costs associated with data breaches. They also have significantly higher costs as compared to other industries. [Read more](#)

July 25, 2019

FEATURED AUTHORS:

[Linn Foster Freedman](#)
[Sean Lawless](#)
[Kathryn M. Rattigan](#)
[Jean E. Tomasco](#)

FEATURED TOPICS:

[Cybersecurity](#)
[Data Breach](#)
[Data Security](#)
[Drones](#)
[New + Now](#)
[Privacy Tip](#)

VISIT + SHARE:

[Insider Blog](#)
[R+C website](#)
[Twitter](#)
[Facebook](#)
[LinkedIn](#)

NEW + NOW

[Business Email Compromises Bilking U.S. Companies Out of \\$301M Per Month](#)

The United States Treasury Department came out with a report last week that concludes that business email compromises (BEC) are costing U.S. companies more than \$301 million **per month**. The report confirms that the two industries hit the hardest by these scams are manufacturing and construction. [Read more](#)

DRONES

[UPS Seeks Certification for Drone Delivery Services](#)

United Parcel Service of America, Inc. (UPS) is seeking permission from the Federal Aviation Administration (FAA) to operate a network of commercial drones for purposes of delivering packages all across the U.S. If UPS's request for certification is granted by the FAA, UPS could be flying drones over people in populated areas, at night, and beyond the operator's visual line of sight. Specifically, UPS is seeking a Part 135 certification under the FAA, which applies to "air carriers and operators." [Read more](#)

PRIVACY TIP #200

[Iranian-Backed Hacking Group Using LinkedIn to Deliver Malicious Documents](#)

FireEye published research last week that it has identified a phishing campaign by APT34, which is known to be a hacking group out of Iran, that all LinkedIn users should be aware of when considering adding a LinkedIn contact. In particular, if you receive a LinkedIn request from someone named Rebecca Watts from Cambridge University, decline the invitation. [Read more](#)

Boston | Hartford | New York | Providence | Miami | Stamford | Los Angeles | Wilmington | Philadelphia | Albany | New London | [rc.com](#)



© 2019 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain ATTORNEY ADVERTISING under the laws of various states. Prior results do not guarantee a similar outcome.