



SMALL
BUSINESS

Understanding How Technology Can Protect and Help Small Businesses Grow and Thrive

August 23, 2017





Rob Elzner

Director, eCommerce



SMALL
BUSINESS



- 7 year eCommerce veteran. Both B2B & B2C online experience.
- Responsible for small and medium business sales effectiveness on Dell.com.
- Prior small business restaurateur.



Agenda:



- **Why online technology and eCommerce capabilities are critical for all small business to grow & thrive.**
- **What technologies should small businesses to be leveraging for themselves and their customers.**
- **What are genuine security threats and how to protect your business.**



Poll Question 1



For which industry is online commerce not important?

- a) Real Estate
- b) Legal Services
- c) Grocery
- d) Manufacturing

A Look Back - 1996



- Average personal computer was around \$2,000
- Only one-third of households had a personal computer.
- Less than 20% had internet access



What Are the Signs Today



- 50%+ of customers prefer to purchase online. Forecasted to grow to 66% by the holiday period in 2018.
- 80% of shoppers in the U.S. purchase online monthly.
- 95% of U.S. adults never have their mobile phone more than 5 feet away at any point in the day.
- Online dating is now the #1 way of meeting new partners.



Websites Alone Are Not Enough



Online commerce is disrupting every industry!





How to Win



To win, grow, and thrive, small business must “digitize” their customer engagements

Traditional Retail / eTail

- Nimble software systems
- Predictive Analytics
- Personalized Content
- Virtual / digital online assistants

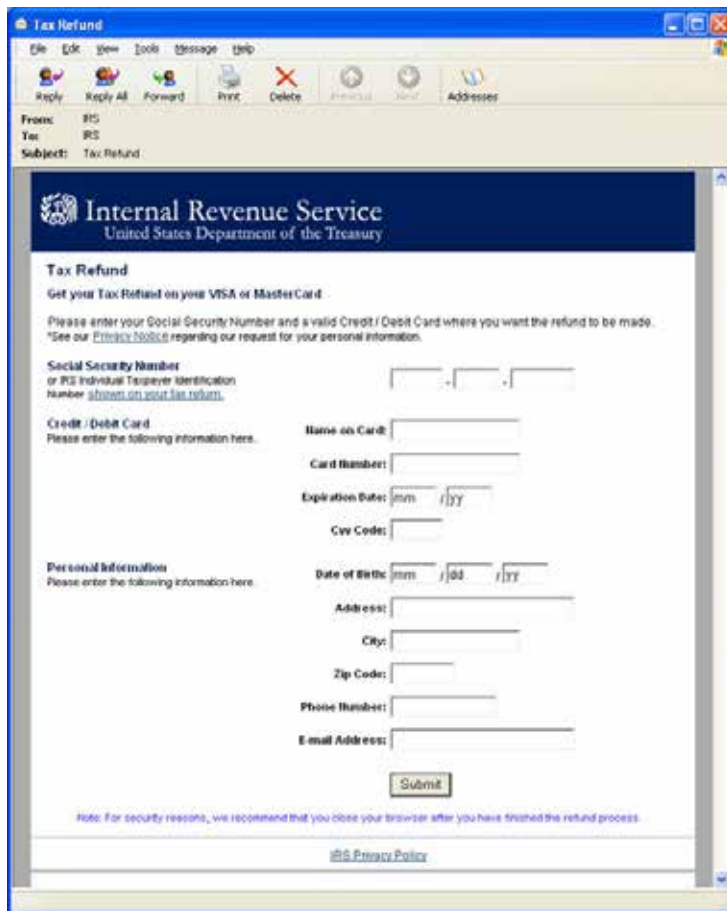
Non-Traditional Retail / Professional Services

- Interactive client portal
- Digital forms and documents
- Online payments
- Video conferencing

Poll Question 2

This is a Phishing scam.

- a) True
- b) False



The screenshot shows an email client window titled "Tax Refund". The email header indicates it is from "IRS" with the subject "Tax Refund". The main content of the email is a form titled "Internal Revenue Service" and "United States Department of the Treasury". The form is titled "Tax Refund" and asks for personal and financial information to receive a tax refund. The form includes fields for Social Security Number, Credit / Debit Card information (Name on Card, Card Number, Expiration Date, CVV Code), and Personal Information (Date of Birth, Address, City, Zip Code, Phone Number, and Email Address). A "Submit" button is located at the bottom of the form. A note at the bottom of the form states: "Note: For security reasons, we recommend that you close your browser after you have finished the refund process." A link for "IRS Privacy Policy" is also present at the bottom.

Poll Question 2



SMALL
BUSINESS

TRUE

Tax Refund

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: IRS
To: IRS
Subject: Tax Refund

Internal Revenue Service
United States Department of the Treasury

Tax Refund
Get your Tax Refund on your VISA or MasterCard

Please provide your Social Security Number and a valid Credit / Debit Card where you want the refund to be made.
Personal information.

The email is not addressed to you. There is no information shown that indicates that the sender knows who you are.

SSN: []-[]-[]-[]

Credit / Debit Card
Please enter the following information here.

Name on Card: []

A "CVV" code is only needed to validate the use of the card for purchases – not deposits.

CVV Code: []

Personal Information
Please enter the following information here.

Date of Birth: [mm] / [dd] / [yy]

Address: []

City: []

No self-respecting organization would ask for this type of information via an email form – it is not safe. This is not a secure web site (using an https connection, it is an insecure email).

Submit

Note: For security reasons, we recommend that you close your browser after you have submitted your information.

There is no other means of contacting the them. This is always a bad sign.

[IRS Privacy Policy](#)

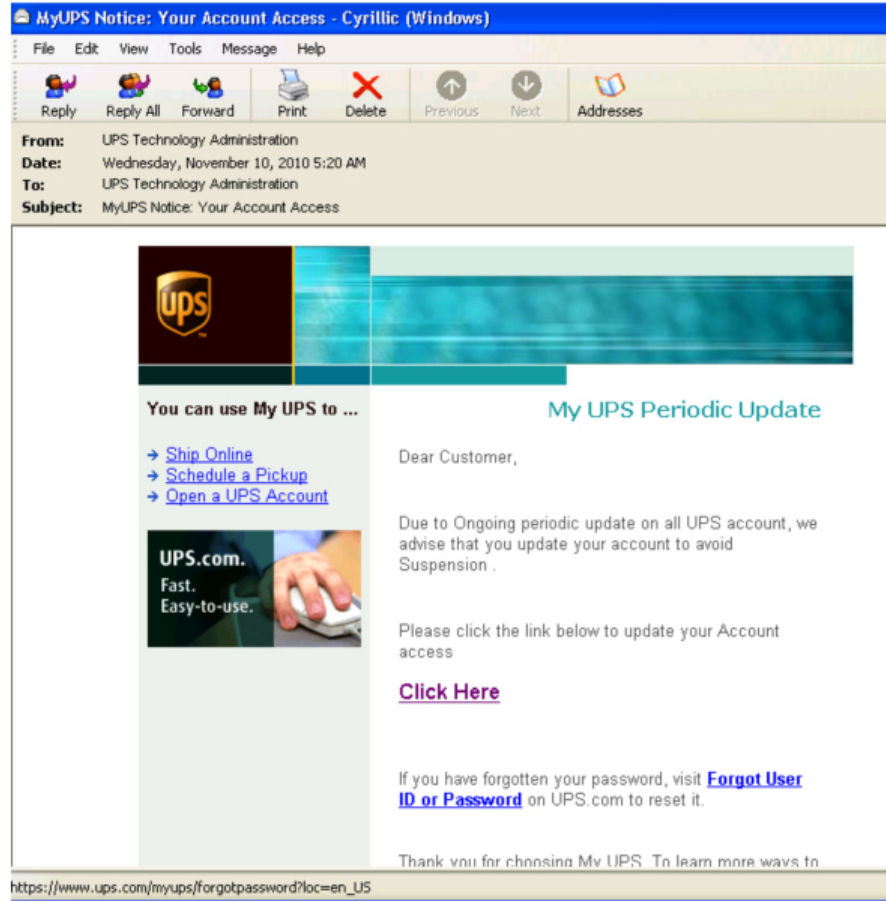
Poll Question 3



SMALL
BUSINESS

This is Phishing scam.

- a) True
- b) False



Poll Question 3



SMALL
BUSINESS


TRUE

MyUPS Notice: Your Account Access - Cyrillic (Windows)

File Edit View Tools Message Help


Reply Reply All Forward Print Delete Previous Next Addresses

From: UPS Technology Administration
Date: Wednesday, November 10, 2010 5:20 AM
To: UPS Technology Administration
Subject: MyUPS Notice: Your Account Access



You can use My UPS to ...

- [Ship Online](#)
- [Schedule a Pickup](#)
- [Open a UPS Account](#)



My UPS Periodic Update

Dear Customer,

Due to Ongoing periodic update on all UPS account, we advise that you have a temporary account suspension.

Please click the link below to update your account.

If you have forgotten your password, visit [Forgot User ID or Password](#) on UPS.com to reset it.

Thank you for choosing My UPS. To learn more ways to

https://www.ups.com/myups/forgotpassword?loc=en_US

Wrong use of casing.

Valid URL is deceiving; most of the URLs in this email are legit except one. So please remember to check all of the links.

The Ransomware Threat



> 140 million new malware variants in 2015.¹

Ransomware is one of the top threats — and it's on the rise. Ransomware damages reputations, drains productivity and costs organizations millions.

390,000 new malicious programs every day.²

400,000 ransomware attempts in 2015.⁵

\$325 million ransom paid by victims in 2015.⁶



Protecting endpoints — the portal to your organization — is critical.

63% of surveyed organizations have had one or more advanced attacks during the past 12 months.³

\$300,000 increase in the average cost of enterprise data breaches in 2015 from 2014.⁴

“On average, small companies lost over \$100,000 per ransomware incident due to downtime. For one in six organizations, these attacks caused 25 hours or more of downtime” - CNN, 2017

What is Ransomware



[Wikipedia](#) defines ransomware as “a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.”

- Can be downloaded onto PC via compromised websites or malicious emails.
- “Ransom” payments can include bitcoin, gift cards (i.e. Amazon, iTunes)
- Paying the ransom does not guarantee resolution.



How to Protect Against Ransomware



- Ensure anti-virus is up to date.
- Back up data regularly. Utilize automated backup and recovery programs.
- Invest in end-point security products and appliances.



Dell Small Business Advisor Campaign



Products



Partnership



Dedicated Sales Team



Financial Services



RAKIA REYNOLDS
OWNER, SKAI BLUE MEDIA



MARIO
SMALL BUSINESS ADVISOR

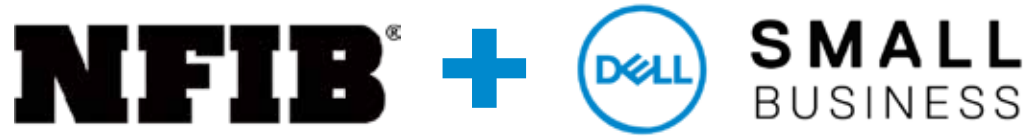


SMALL
BUSINESS

Dell / NFIB Association Program



www.dell.com/NFIB



- Exclusive discounts. **38% off** business PCs and Servers
- Free consultation from highly trained small business technology advisors.



SMALL BUSINESS

THANK YOU !



Contact info



Robert.Elzner@Dell.com



[linkedin.com/in/robert-elzner-810608](https://www.linkedin.com/in/robert-elzner-810608)



[@rse3454](https://twitter.com/rse3454)

