Five Actions to Take to Improve your Shop's Cybersecurity

Michael Boucher – FTD Sr. Director, Information Risk Management

April 17, 2018

SOCIAL NETWORKS
GLOBAL ECONOMY
EXPOSURE
E-MARKETING
COMMUNICATION
MARKETS
INFORMATION TECHNOLOGY
ADVERTISING
PROMOTION
COMPUTER
WWW
SOCIAL MEDIA
BIG DATA
CONTENT
TARGET
CODING
SOFTWARE
SOCIAL
SERVICES
CONSUMER
CONSUMER DEMAND
MULTIMEDIA NETWORK
PROJECTS
ORGANIZATION
WEB MARKETING
APPS
STATISTICS
GROWTH
INTERNET
ADVANCES
PROGRAMMING
HACK
BRANDS
SOLUTIONS
WEB
HACKING
VIRAL
DATA
MARKETING
BUSINESS
VISION
ENGINEERING
COMMUNICATION
METRICS
SOCIAL
PLANNING
WEB DEV
BRAND
WEB SERVICES
PROJECTS
BIG
SERVICE
STRATEGY WORLDWIDE
BUZZ
DATA
ORGANIZATION
BEHAVIOUR
PRO
CODING
PRICING
NEXT GENERATION
MEDIA
MOBILE
MEDIA
PLANNING
INFORMATION
SOCIAL NETWORKS
ANALYTICAL THINKING
DIGITAL

Why is Cyber Crime Such a Problem?

It's Easy to Do

Anonymous Crime

Low Risk Crime

It's Very Profitable

Threats Evolve Quickly

Social and Political Influence

1. Keep Work and Personal Computers Separated

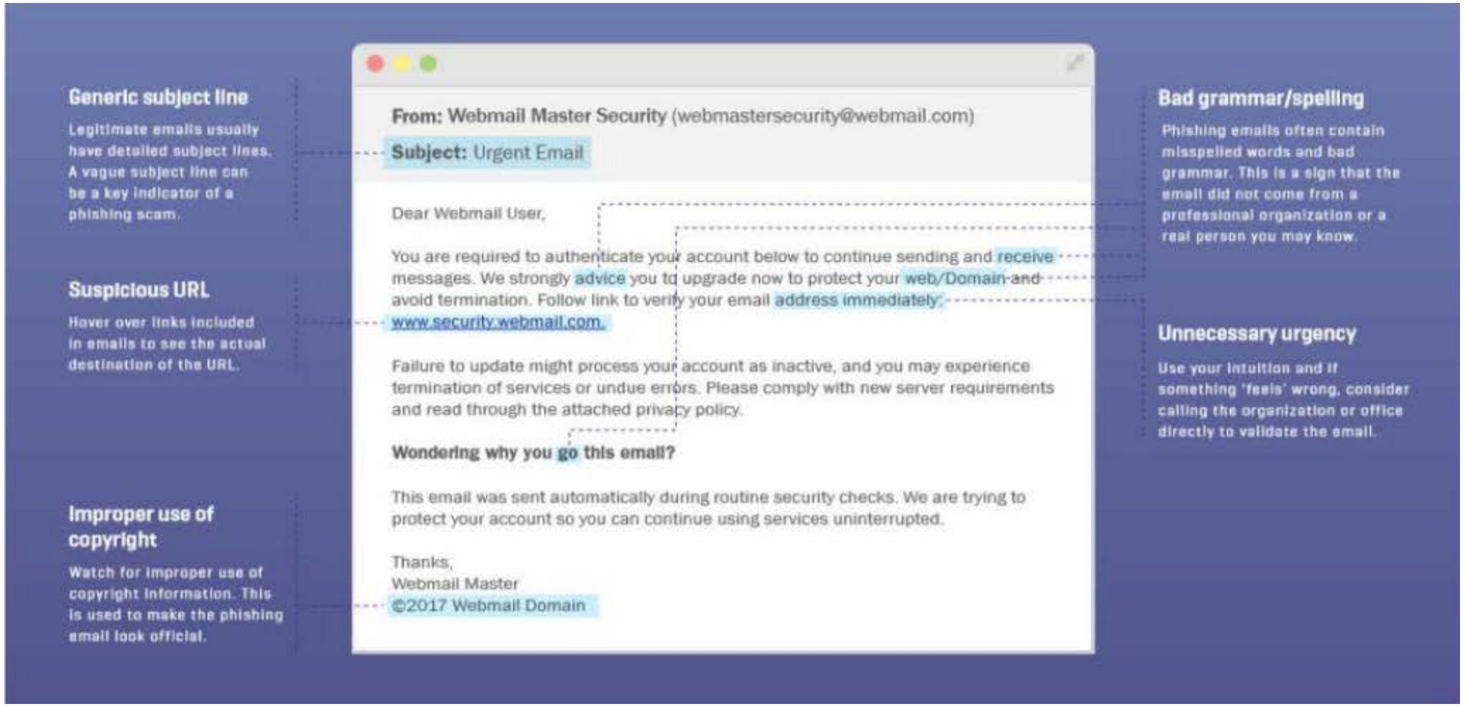
- Use a dedicated computer for processing orders and point of sale systems. Use a separate computer for email and Internet browsing.
- Reduces the risk of critical systems being infected by ransomware or other computer viruses.
- Ransomware and computer viruses may cause all systems in the shop to stop working.
- Use caution in transferring files between computers using a USB drive. Computer viruses can move to other computers via USB drives.

2. Phishing

Think before you click:

- Do not open email attachments that you were not expecting, or click on links on suspicious websites.
- Delete emails that try to get you to open an attachment to receive something like money or a parcel. This is likely an attempt to get you to install bad software.

How to Spot a Phishing email



Generic subject line

Legitimate emails usually have detailed subject lines. A vague subject line can be a key indicator of a phishing scam.

Suspicious URL

Hover over links included in emails to see the actual destination of the URL.

Improper use of copyright

Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately: www.security.webmail.com.

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

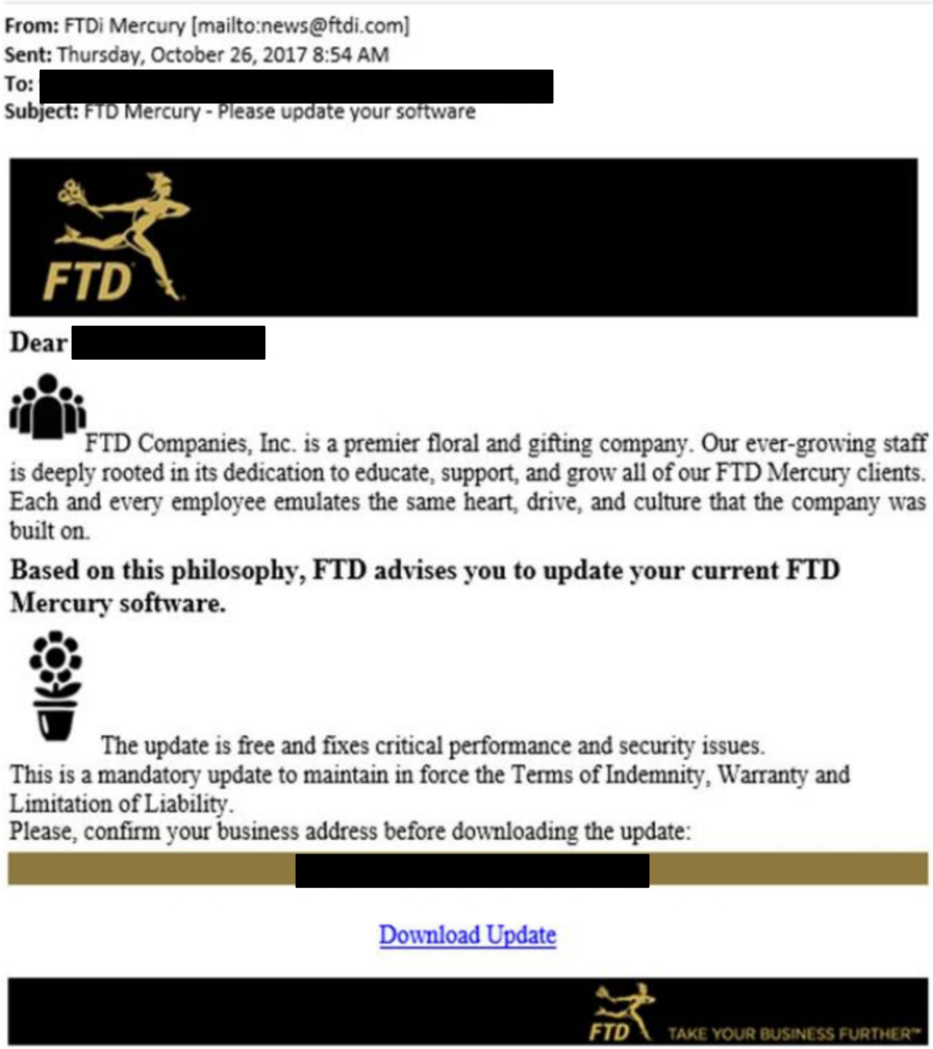
Bad grammar/spelling

Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

Unnecessary urgency

Use your intuition and if something 'feels' wrong, consider calling the organization or office directly to validate the email.

FTD Phishing Example



From: FTDi Mercury [mailto:news@ftdi.com]
Sent: Thursday, October 26, 2017 8:54 AM
To: [redacted]
Subject: FTD Mercury - Please update your software

Dear [redacted]

FTD Companies, Inc. is a premier floral and gifting company. Our ever-growing staff is deeply rooted in its dedication to educate, support, and grow all of our FTD Mercury clients. Each and every employee emulates the same heart, drive, and culture that the company was built on.

Based on this philosophy, FTD advises you to update your current FTD Mercury software.

The update is free and fixes critical performance and security issues.
This is a mandatory update to maintain in force the Terms of Indemnity, Warranty and Limitation of Liability.
Please, confirm your business address before downloading the update:

[redacted]

Download Update

Attacker sent a well crafted phishing email message to florists and FTD employees to trick them into clicking on a link that would make their computer vulnerable to future attacks.

Key Take Away Points

- FTD and our florists are a target.
- Florist systems are particularly vulnerable, and a successful attack could have a serious impact on customer orders.
- FTD is developing a security awareness campaign for our florist members to inform and guide them on security issues.
- Improve technical controls (e.g. patching and anti-virus) to reduce the risk of system compromise.

3. Patching

Stay up-to-date:

- Make sure that all of your security programs operating system are up-to-date.
- Enable automatic updates to improve the update process.
- Consult FTD support. Not having current FTD Mercury software could cause an interruption to your service.

4. Anti-Virus

Secure your PC:

- Anti-virus software scans your computer's memory for certain patterns that may indicate the presence of malicious software.
- It can detect and block many viruses before they infect your computer.
- It can only identify known malware. New viruses may not be detected.
- New malware is identified daily, which is why it's critical to update your anti-virus regularly.

5. Backup Your Files

Always backup your data:

- There's always a possibility of losing your data from ransomware or other technology failure.
- Develop a backup program.
  - What should I backup?
  - How often should I back it up?
  - How long should I hold the backup?
- 3-2-1 Backup strategy
  - 3 copies of your backed up data
  - 2 copies on different media (e.g. flash drive, cloud storage, etc.)
  - 1 copy off site (e.g. copy at home)

FTD Support

888.309.2244

Monday thru Friday 7:00 am – 8:00 pm CT

Saturday 7:30 am – 6:00 pm CT

Q&A