CYBER SECURITY: ARE YOU SECURE? THREE TOOLS TO PROTECT YOUR BUSINESS



PARKER SMITH & FEEK An @@ Company

BEIJING

PORTLAND

SEATTLE

WASHINGTON, D.C.

NEW YORK

SPOKANE







Security Incidents and Data Breaches

- What's the difference between a security incident and a data breach?
- How to respond to a security incident.
- How to respond to a data breach

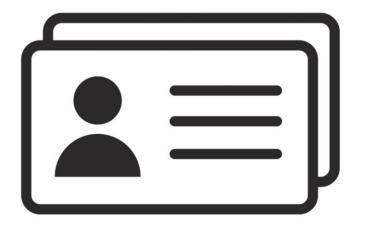






Examples: Point of Sale

- PCI DSS
- Attorney General enforcement actions





FEEK



Social Engineering

- Phishing
- Smishing
- Vishing
- Spear phishing/Whaling



Examples taken from FTC.gov and microsoft.com

PARKER

& FEEK

Your account is on	hold.
Please upo payment d	
ti Dear,	
nformation. We'll try	rouble with your current billing again, but in the meantime yo your payment details.
UPDATE ACCOUNT	WOW
leed help? We're he lentre or contact us	are if you need it. Visit the <u>Help</u> now.
Your friends at Net	flix



Ransomware – Trends

- Statistics
- Recent changes

PARKER

& FEEK







Ransomware – Resources

- The FBI is on your side.
 - https://www.ic3.gov/
 - https://www.cisa.gov/stopransomware



- NISTIR 8374: Ransomware Risk Management: A Cybersecurity Framework Profile
 - <u>https://csrc.nist.gov/projects/ransomware-protection-and-response</u>
 - https://www.nist.gov/itl/smallbusinesscyber



Business Email Compromise

Identifying a Target

Step 2:



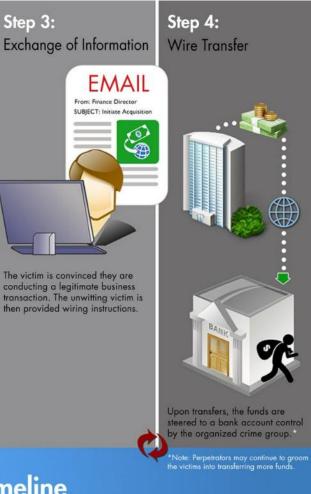
Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.



Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.



Taken from FBI.gov

Business Email Compromise Timeline

An outline of how the business email compromise is executed by some organized crime groups

8



Preparation

- Data mapping
 - Take inventory of the types of data being created, collected, used, stored, and/or disclosed, including PII.
 - Classify data in connection with relevant laws; segregate data.
- Data minimization: If you don't have it, it can't be taken from you.
- Data disposal/destruction (RCW 19.215.020)
- Vendor management





Minimize Risk

- Backup data, system images and configurations.
- Test that backups are saving and keep them offline.
- Use multi-factor authentication.
- Update and patch systems.
- Make sure security solutions are up to date and running.
- Review and test your Incident Response Plan.





Preparation Part 2 – Recovery

- Incident response plan
- Business continuity plan





FEEK

Preparation Part 3 – Insurance Coverage

- Different types of coverage
- Policy requirements:
 - Multifactor authentication (MFA)
 - 3-2-1 method
 - Employee training
 - Patch management
 - Endpoint detection and response





How Prepared are you?

- Today's takeaways
 - Mitigate Risk
 - Recovery

PARKER

& FEEK

Risk Transfer



Contact Us





Eva Novick Foster Garvey PC eva.novick@foster.com 503.553.3163

Lynsee Wiegand Parker, Smith & Feek Lrwiegand@psfinc.com 425.974.3048



PARKER

& FEEK



QUESTIONS





