

CONNECTING THE DOTS

ADVICE FROM THE EXPERTS:
CYBERSECURITY IN OUR NEW (VIRTUAL)
REALITY FROM SAFETY NET

Presenters



Tim Cerny
CEO



Eric Anderson | MCSE, GCIH, CCNA
Sr. Network Engineer

What is IT Security?



Integrity

The data has not been modified and is accurate and complete

Confidentiality

The data is disclosed only to authorized users

Availability

The data is ready and accessible by authorized users

Layered Security Approach

- Anti-virus Software. Typically 50% effective
- Spam Prevention and virus detection
- Web Content Filtering, multiple layers
- Security Patch Management
- Device encryption
- Physical access restrictions
- Next Generation Firewall with IDS and Geo-IP Filtering
- Authentication controls, including two factor auth
- **HR Policy can't be understated**

Real-world incidents





Remember how modern malware acts.

- Lays quietly
- 75% are keyloggers
- Harvest the network, or sell access to infected computers to someone else

Determine your requirements

High Security/Compliance

- Personally Identifiable Information (PII)
- Protected Health information (PHI)
- Homeland Security/Defense (NIST)
- Criminal Justice Information (CJIS)
- Financial records, others

Business-Level Security

- Intellectual property
- Business transactional data
- Not as sensitive, but valuable

The essentials still apply – more than ever

DOWNLOAD THE CHECKLIST

Safety Net Cyber Security Checklist

Our Safety Net IT experts have made the ultimate Cyber Security Checklist for individuals or businesses. You can use this checklist in two ways:

- OPTION 1** Click here for 100 questions, and calculate your score. The test score is 400. A score below 300, or several missing check marks, indicate the need for improved security.
- OPTION 2** Use the assessment as a general guide for your staff or your IT team to make sure it's working about the same as you get protected.

Overarching Best Practices

- Do you have a written disaster plan for all of the following? Available use, Internal Access, Remote Access & IP Addressing, Mail, Data Backup, Cloud Services, Business Recovery, Encryption & Passwords per your level.
- Do you use modern, vetted, and up-to-date software for all personal and organizational devices (OS, apps)?
- Do you hold regular employee training that covers the latest in data security (OS, apps)?

User Security

- Do you require regular updates, antivirus, and screen passwords?
- Do you require password and device locked accounts?
- Do you avoid third-party apps and passwords?
- Do you inspect all email attachments and links when sharing sensitive information or passwords?

Email Security

- Do you have an email security filtering tool or a filtering solution in place against malicious email attachments?
- Do you use email policies that limit an email recipient's ability to view attachments, passwords, banking info, or anything else that safety cannot be used over the phone.

Website Security

- Is your Web application protected?
- Do you use a secure web hosting company? Do you have secure hosting services, firewalls, server logs, and backup your site regularly?

Network Security

- Do you have a commercial grade firewall?
- Do you perform a patch your router and your internal Wi-Fi access to be employees and IT staff get internet connections?
- Do you use VPN to mask your internet technology for remote access to the office?
- Do you use intrusion vulnerability test the network and require logging back in after a period of inactivity?
- Do you limit and log access to the physical location of network equipment, network devices (switch, routers, and firewalls) and any in-house servers?
- Do you have data security in cloud software using password and protection for accessing the data?

Ask an IT Expert

- Are your IT services using the best security tools, considered top generation updates, and delivered by the best talent with the right education or training support?
- Do you require your staff to receive the best security training, updates, resources, and the support and device?
- Do you have personnel an emergency contact?
- Do you perform regular backups of data and all programs, as well as the website?

How did you check out? Is it not clear about your security and/or things to do, visit the Safety Net blog at safenet.com/blog.

If your business is in the Washington DC Metropolitan Area, call 800-850-8500, your local Safety Net can provide managed IT services and help you get a service for a healthy IT environment. Contact us today! Remember, IT is the most important part of your business, not just a tool.

YOUR TOTAL:

safenet-inc.com/checklist

Email is not secure

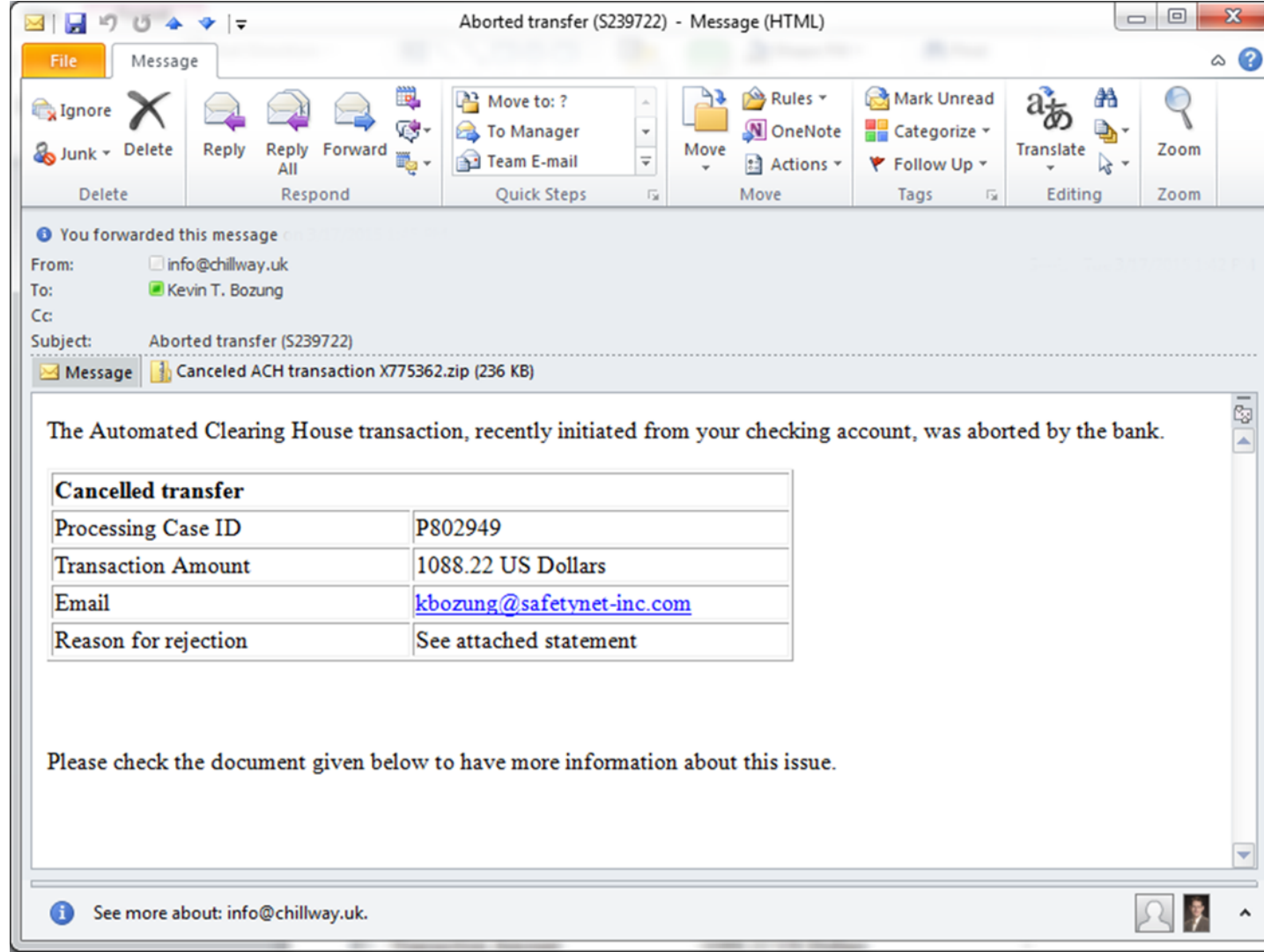
- Don't email passwords, SSNs, or other sensitive information
- Use secured file sharing



Phishing Attacks (malicious spam)

- 49% of all email is spam
- Spear phishing
 - Disproportionately aimed at small businesses
 - Highly targeted





Video Conferencing Platforms

Go business-grade

- GoToMeeting
- MS Teams or Skype
- Cisco Webex
- Zoom, post-security fixes

Use smart passwords

Manage and enforce software updates



Other things to check on

1. For computers being used remotely, how are anti-virus and OS updates being monitored and remediated?
2. Who's checking integrity and consistency of data backups?
3. What amendments are needed to our remote work policy in this situation?
4. How are our customers' credit card data being handled right now?
5. Are all remote workers up to date on security awareness training?

Q & A

Contact information for the presenters:

info@safetynet-inc.com

(231) 944-1100