Restech

User Security

AVOIDING LOSS – GAINING CONFIDENCE IN THE FACE OF TODAY’S THREATS
Your presenter:

Vince Gremillion, CISSP

- 30+ years technical and customer service experience
- Founder/Co-Owner RESTECH Information Services
- 2013 Louisiana Small Business Person of the Year
- Implemented ISO 27001 security protocol
- Implement and manage ALTA/TRID regulation
What to Expect?

- As an **USER, OWNER, MANAGER or EXECUTIVE**
- Understand the **CRITICAL INFORMATION ASSETS** and threats against them
- Learn the basics of an **EFFECTIVE SECURITY PROGRAM**
- Data security is everyone's responsibility – not just IT
- You as the **Data Handler** – The most critical part of any security plan
- Learn the habits of security
- It’s not about hackers – it’s about you!
  - Users leak and lose more data than hackers ever steal.
  - Poor data handling habits are a leading cause – data sprawl,
"I'M NOT AFRAID"

"YOU WILL BE. YOU.WILL.BE."

FOR ALL LAW FIRMS
Cybersecurity should be JOB #1

WHY?
Because you handle confidential data and secret information that belongs to your clients, not you. It is your ethical duty to protect this information!

-- see Rule 1.6 of the ABA Model Rules of Professional Conduct

Cybersecurity is not an IT problem it's a BUSINESS PROBLEM

% OF LAW FIRMS
86%
NOT USING
TWO-FACTOR IDENTIFICATION

% OF LAW FIRMS
78%
NOT USING
ENCRYPTED EMAILS

% OF LAW FIRMS
58%
NOT USING
ENCRYPTED LAPTOPS

% OF LAW FIRMS
76%
NOT USING
ENCRYPTED USB DRIVES

% OF LAW FIRMS
64%
NOT USING
INTRUSION PREVENTION

SO WHAT?
Current news/threats

RANSOMWARE

PHISHING & SOCIAL ENG.

INTERNAL THREATS

LOST / STOLEN DEVICES
More likely threats?

- **Weak security of others who handle your data** – Equifax, Yahoo et al
  - Non-Profit groups, churches, sports, associations are soft targets

- Account takeover - Lack of validation for password resets (IRS, PayPal and many others)
  - Using the same password across many accounts

- Banks take email to authorize wires
  - Know how your vendors can pose a risk

- Entire supply chain is at risk - software libraries, firmware, Chinese mfg.

- USB thumb drives
9 POINTS OF SECURITY

1. Password & Account Security
2. Patches and Updates
3. Data Protection
4. Permission Management
5. Physical Security
6. User Awareness Training
7. Malware Protection
8. Email / Web Security
9. Business Continuity
Passwords and Account Security

- Change **default passwords** immediately on any connected device (if you can*)

63% of confirmed data breaches leverage a **weak, default, or stolen password**.

Source: 2016 Data Breach Investigations Report from Verizon

www.insecam.org
1. **Passwords and Account Security**

- Change **default passwords** immediately on any connected device.
- Use more than UPPER / lower case and numbers.

2. **Possible characters**

   - **BASE**
     - 52 UPPER & lower characters in the alphabet
     - +10 Numbers
     - +30 Special characters such as `[]/<>,.%^%$#@!?~`
   - **EXPONENT**
     - 92 Possible characters

3. **63%** of confirmed data breaches leverage a **weak, default, or stolen password.**

   Source: 2016 Data Breach Investigations Report from Verizon
Change default passwords immediately on any connected device

Use more than UPPER / lower case and numbers

Passwords should be replaced with long pass phrases greater than 10 characters

i-L0v3-this_te@m! | L0ze*>15#Bye2018

63% of confirmed data breaches leverage a weak, default, or stolen password.

Source: 2016 Data Breach Investigations Report from Verizon
Get and use a Password Vault or Single Sign On product
Couple it with 2 Factor Authentication

63% of confirmed data breaches leverage a weak, default, or stolen password.
Source: 2016 Data Breach Investigations Report from Verizon

1Password
Dashlane
Okta
Duo
Keeper
LastPass
Yubico
SaaSPass
Passwords and Account Security

- Change **default passwords** immediately on any connected device
- Use more than UPPER / lower case and numbers
- Passwords should be replaced with long pass phrases **greater than 10 characters**
- Consider a **password manager** for daily use protected by a super complex passphrase
- If one site is hacked and you share passwords, **all sites need to be changed**
- Activate 2FA (2 Factor Authentication)
- NEVER have passwords written on paper around your desk!!!! Can be stored securely somewhere else.
- HAVE I BEEN PWNED? www.haveibeenpwned.com

63% of confirmed data breaches leverage a **weak, default, or stolen password.**

Source: 2016 Data Breach Investigations Report from Verizon
Patches and Updates

“Zero day” exploits attack flaws in most software

Apply patches ASAP

Don’t expose systems directly to the internet

- Flash
- Adobe
- Windows
- Java
- Firmware in hardware
- Cameras
- TVs
- IOT (internet of things) – anything connected to Internet: home automation, entertainment, security, cars, toys, etc
Data Protection – a reputation and liability issue

The data on your systems is often more valuable than the system or business itself

- User errors
- Accidental deletion
- Intentional deletion
- Storms or floods
- Cyber attacks
- Power outages
- Electronic failure
- Stolen equipment
Data Protection – a reputation and liability issue

What is the required **TIME TO RECOVER** your lost data?

A GOOD DATA PROTECTION SYSTEM:

- Backed up **locally and offsite + encrypted**
- Contains **many versions**
- Recovers data or systems **fast**

**FAST DATA RECOVERY IS THE RESULT OF A WELL-DESIGNED BACKUP SYSTEM**

- Attached disks and NAS are vulnerable
Permissions

Users
YOUR PEOPLE

Roles
THE FUNCTIONS
OF YOUR USERS

Permissions
APPROVED
AUTHORIZATIONS
FOR EACH USER

Knowing who has access to what is a basic security function for asset owners.
How Do You Secure Your House?

PROTECTION | DETECTION | RESPONSE
Physical Security

Anticipate avenues of attack and prepare

- Locked doors
- Lighting
- Access control
- Badges
- Employee screening
- Personal Security

- Logs
- Cameras
- WIFI
- Open ports
- Documents on desk, in car
Awareness

Everything depends on this

- Owners, Executives, and Managers have to **lead by example**
- Awareness training is a **cultural shift**
- Nearly all breaches can be traced to a **human exploit**
- The value of the data is far greater than the equipment it is on.
- The exposure to liability and loss of reputation are the greatest risks to handling data.
Awareness

Everything depends on this

▶ Don’t click links from unsolicited Email
▶ Type them into browser or use your Bookmarks
▶ Hover mouse over a link to confirm
▶ Verify the sender – but not by replying to that email.
▶ Be careful of Outlook autofill addresses
▶ Disposing of data – secure deletion, not in MY DOCUMENTS
  ▶ Develop and work within a policy/procedure framework
Awareness – threats are following you

More Vulnerabilities than Ever!

Digital records everywhere

Conveniences

Everything Always ON
always connected

Cloud services

META Data

“SMART”
devices

Social Media

Smart Phone

Online everything

Cameras
Awareness – spot phishing email

Unsolicited – When in doubt – DELETE!

Spelling

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form:

http://www.facebook.com/application_form

Links in email

Note: If you don’t fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department

Popular company

Threats

https://www.woodgrovebank.com/loginscript/user2.jsp

Malware Protection

Don’t “cheap out” here

► Do not jeopardize the security of your business by relying on “free” virus protection

► Improper configuration and lack of updates will make any product useless

► Better products detect known and unknown threats – it’s worth the expense
Email & Web Security

Protect the ENTRY and EXIT points

- Email and Internet – main avenue of cyber attacks and misuse of data
- Active filtering firewall – limit egress
- Email spam protection
- Accurate SPF records to reduce spoofing
- You need reporting to see what is being used by who
- Prevent accidental access
Business Continuity

Planning for the unexpected

- Anticipate what can happen and what affect it can have
- Ultimate deliverable for your IT service provider
- Downtime costs much more than hourly service savings
Protecting Yourself
- Activate **alerts** on your accounts
- Activate **Two Factor Login**
- Use **Positive Pay** services
- **Freeze** your credit accounts
- Reconcile your own accounts
- **Dual Signature** where you can
- Do not use PC/email to authorize wire transfers
- Limit exposure of personal data on social media
- Avoid Public WIFI without a VPN service
- Change your passwords
- Delete old accounts
CALL TO ACTION

Contact RESTECH to schedule:

- Phishing test
- Network assessment
- Cybersecurity consultation

(504) 733-5633

www.restech.net
EMAIL: info@restech.net