

BANKING SERVICES



WHY FRSECURE?

FRSecure is contracted by banks to perform e-mail phishing attacks on the bank's employees.

In 2013, FRSecure succeeded in breaching 100% of our banking clients with e-mail phishing.

Approximately 65% of targeted bank employees provided login credentials to critical systems during the attack.

Regular training and awareness is critical to managing exposure to phishing and other social engineering tactics. Could you be one of the 65%?

BEFORE SECURITY BECOMES YOUR CUSTOMER'S PROBLEM

GRAMM-LEACH-BLILEY ACT (GLBA)

We are experts with section 501(b) of GLBA and the Interagency Guidelines establishing Information Security Standards (12 CFR 364, Appendix B) as each pertains to information security.

INFORMATION SECURITY AUDITS

**Are security audits something you just check off your list of things to do?
Are you getting any real value from your investment?**

FRSecure's Security Experts receive the highest marks from our clients for their thorough and friendly approach to:

- Ensuring you fully understand your security compliance requirements
- Assessing and measuring your risks
- Providing an appropriate, prioritized security road map
- Presenting easy-to-follow, yet comprehensive reports
- Communicating findings to auditors and leadership
- Building effective security programs

EXTERNAL VULNERABILITY ASSESSMENT

Where are you vulnerable to attacks via the internet? Regularly scanning for vulnerabilities is important, but only a half-measure.

FRSecure employs a wide range of tools to find and verify your external vulnerabilities. We also search the internet for information that might have leaked via social media or other means. Our security experts interpret the results and provide you with documentation and recommendations to better protect yourself.

SOCIAL ENGINEERING

How vulnerable are you to e-mail phishing or impersonation attacks?

Find out by partnering with FRSecure. Leverage our experience to put your bank to the test in a controlled environment. Afterward, we will utilize the exercise to facilitate meaningful, relevant training and awareness for your team.

GET THE PICTURE

FRSecure's reporting paints a clear, easy to understand picture of your risks. Many "security companies" trying to evaluate security programs lack the experience and expertise to make appropriate recommendations that genuinely improve security for their clients. FRSecure client feedback on our reporting, process and recommendations is overwhelmingly positive.

DON'T FORGET

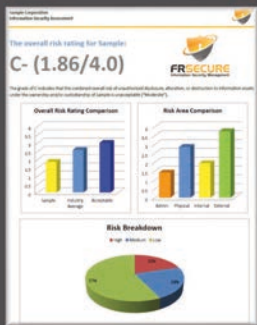
PCI-DSS: Accepting credit cards anywhere in your organization means you have requirements to comply with the Payment Card Industry (PCI). FRSecure offers a Certified PCI Professional (PCIP), PCI Qualified Security Assessor (QSA) designation and decades of PCI experience on staff.

Breach Response: Experiencing a breach to your systems or personnel? Engage FRSecure to develop an effective and appropriate response and a plan for your future protection.

Disaster Recovery: Minimizing data breaches is important, however deletion or corruption of your information can negatively impact your organization in unrecoverable ways. Preparation is key to ensure you can recover from the unthinkable. FRSecure can help.

SOUND FAMILIAR?

We change our security auditors every few years. This is a good idea, but how do you know you're getting an apples to apples assessment of your information security program when you change vendors. FRSecure can help you build your program on an open information security standard, such as ISO. Now rooted in a well-known standard, your security program won't need reinventing with each new security vendor. We're a small bank, we don't need big security. You're right! There is an appropriate level of security for every bank. FRSecure will help you find the appropriate level of security based on your needs.



DOCUMENTATION:

Executive Summary with easy to understand breakdown

OUR SERVICES

- GLBA Security Assessments
- General Controls Assessments
- Information Security Risk Assessments
- PCI-DSS QSA
- Penetration Testing
- Social Engineering
- IT Vulnerability Assessments
- Security Program Development
- Disaster Recovery
- Breach Response
- Policy Development
- Training and Awareness
- ISO Gap Analysis

