



Identity Theft – Threats

Cezary Prokopowicz

RSA Security, CEE Territory Manager

Threats and Points of Exposure

Passwords are not secure

- Existing passwords have been proven to easily be compromised
- Unrealistic burden placed on end users by multiple passwords
- Challenge of remembering so many different words and numbers is already hindering online commerce

Phishing attacks proliferate

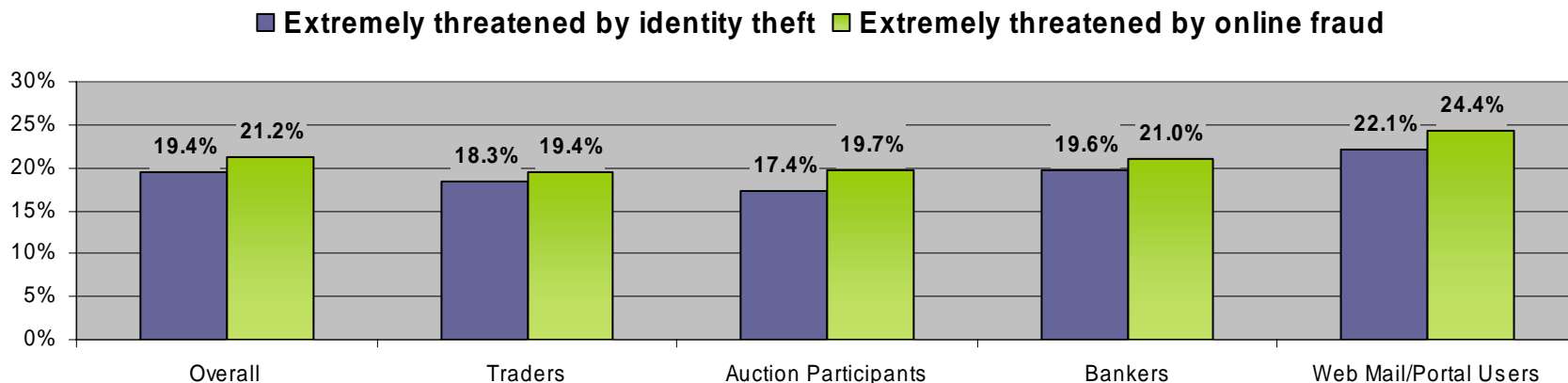
- 2,870 active phishing sites were reported in March alone—an **increase of 28% a month**
(Source: Anti-Phishing Working Group)
- Nearly **1.6 million U.S. consumers were defrauded** via phishing between May 2004 – May 2005
- This cost banks and card issuers more **\$2.1 billion** in losses (Source: Gartner)

Toll on Consumer Security Perceptions

When asked...

“How threatened do you feel by online identity theft and online fraud?”

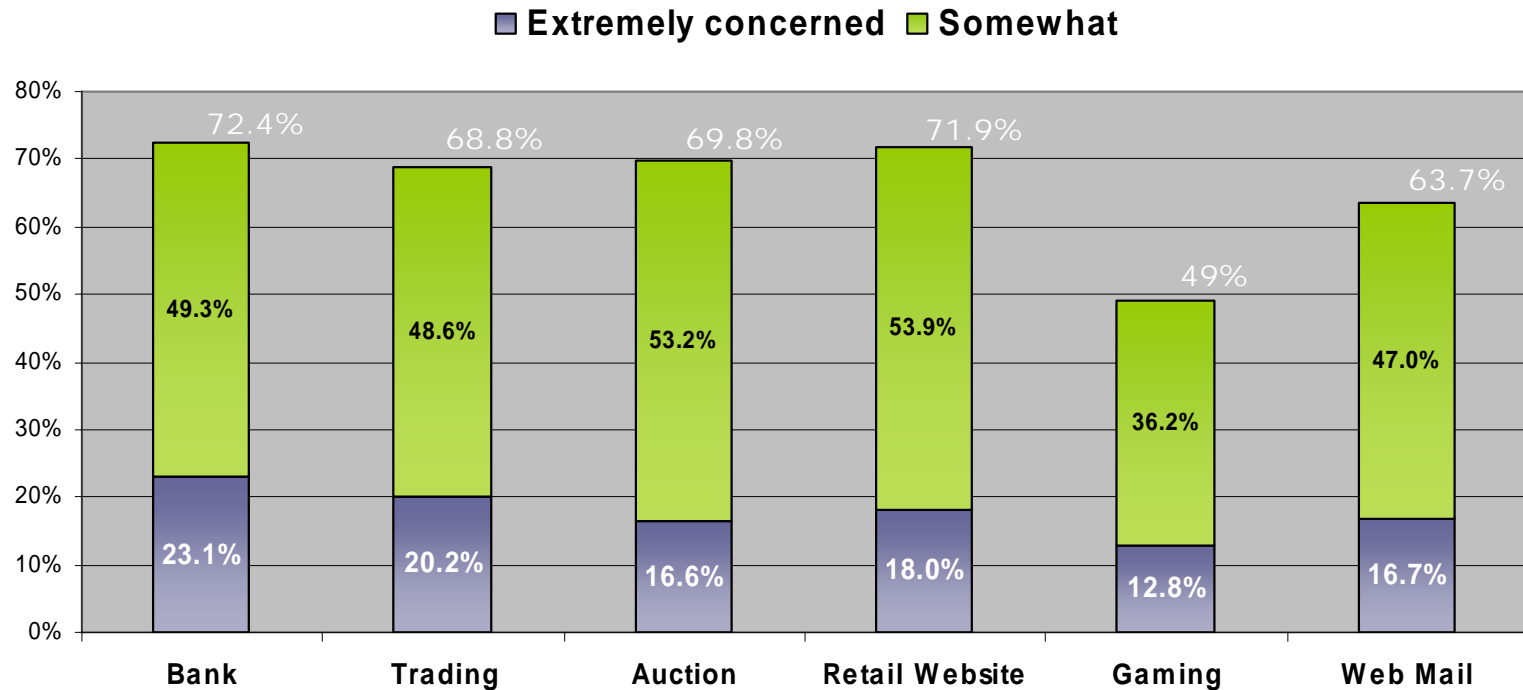
...one-fifth of all consumers felt extremely threatened.



Toll on Consumer Security Perceptions

When asked...

“How concerned are you that someone will fraudulently access your online [XX] account?”
...two-thirds of all consumers felt concerned.



Toll on Consumer Behavior

Lack of confidence in transacting online

Of online consumers, identity theft concerns have convinced...

- 35% to not enroll or use online banking or bill payment
- 41% to not apply online for a financial product
- 33% to not shop online with a credit card

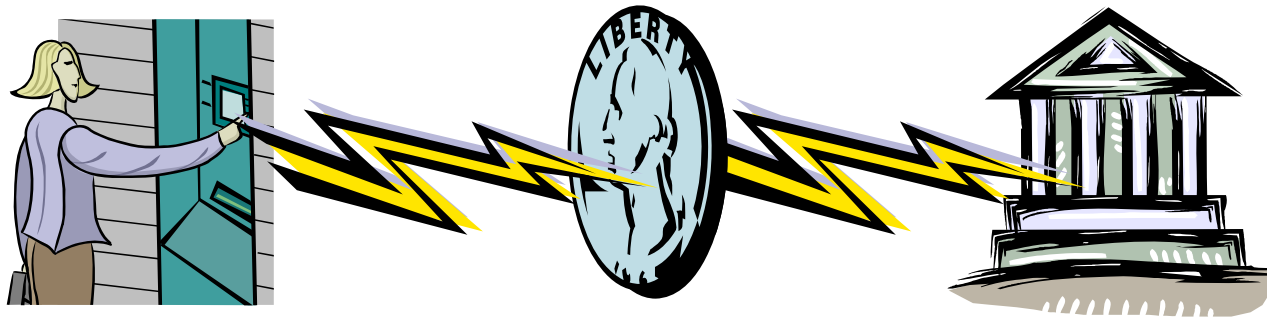
(Source: Forrester Research)

What is Phishing?

Two sides of the same coin...

Identity Theft

Phishing

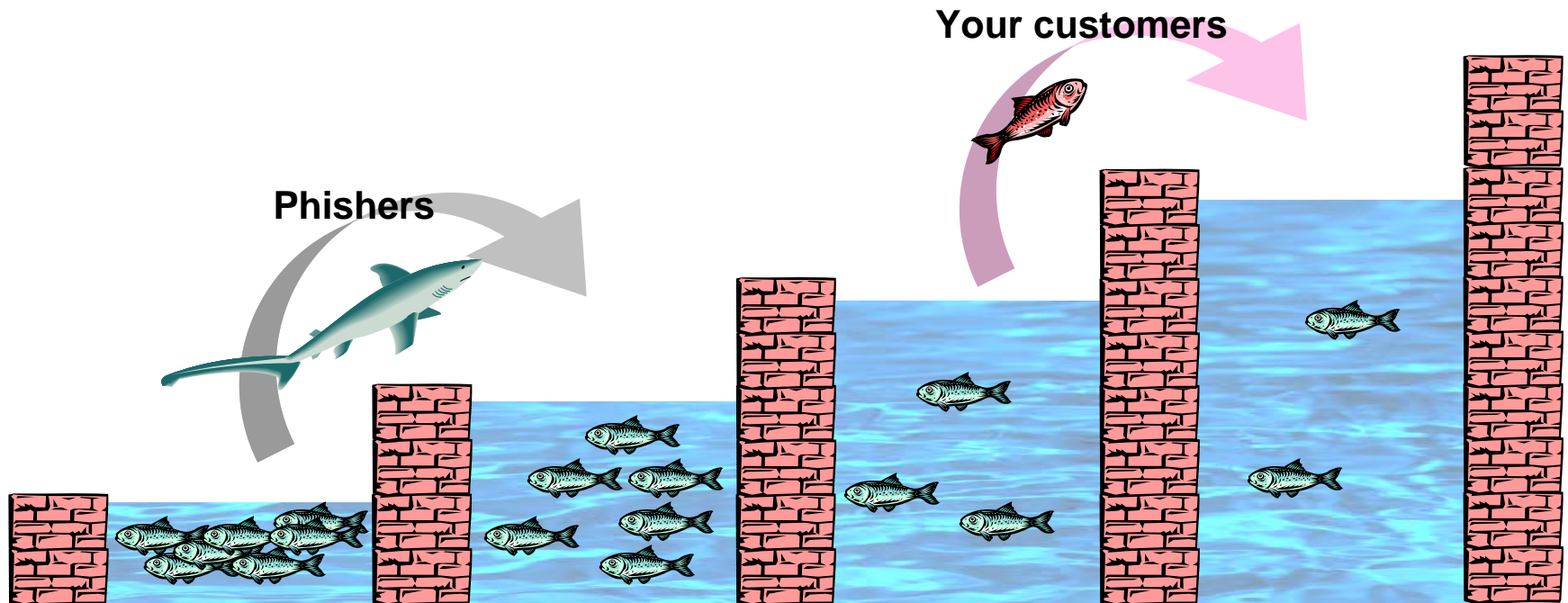


**When a user's
identity is stolen**
*to commit a fraudulent
transaction*

**When the bank's
identity is stolen**
*to solicit private
information from users*

Phishing is a Dynamic Practice

"You don't have to swim faster than the shark.
You just have to swim faster than the other fish."



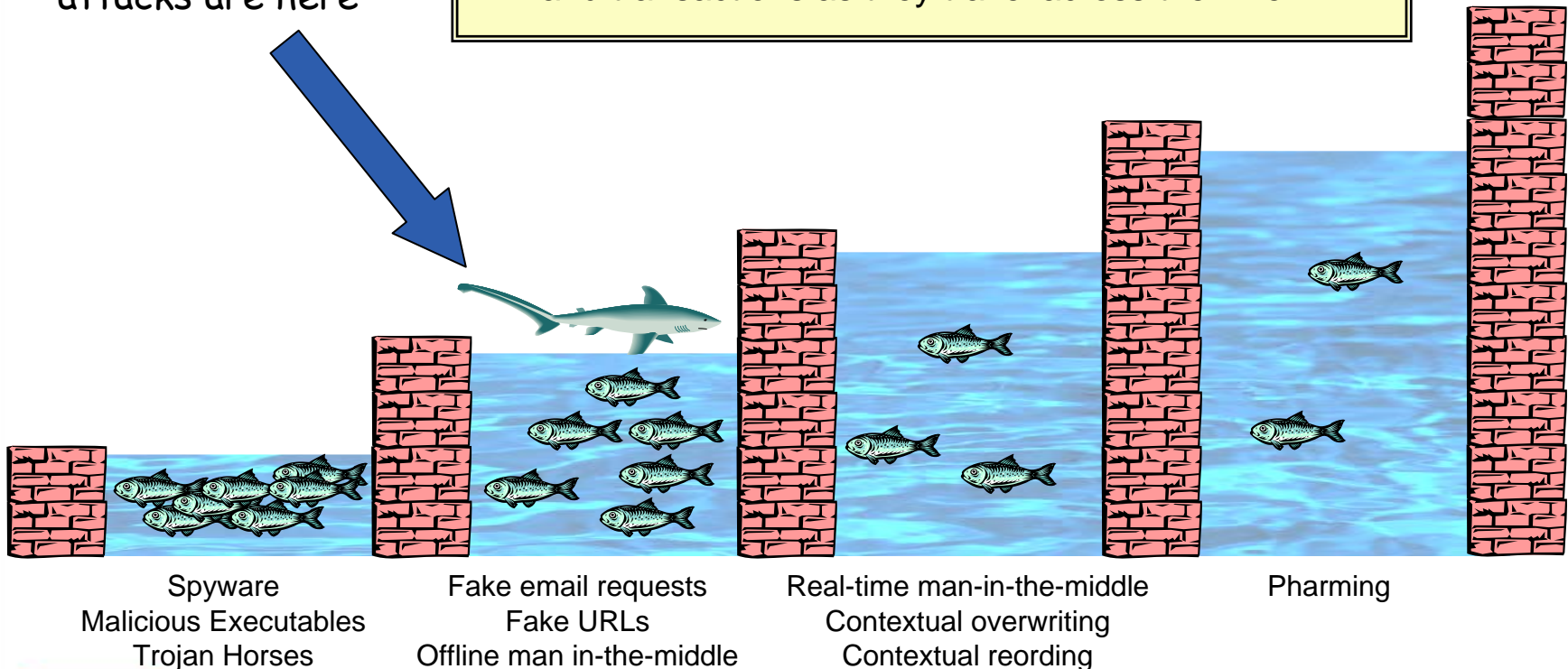
- Phishers build their systems to carry out a particular style of attack, targeting the easiest prey
- Avoiding the phishers requires moving beyond the scope of their chosen attack styles.
- The phisher would rather find other easy targets than invest in "jumping the wall" to the next level of sophistication.

Common Phishing Techniques



Today, the most common phishing attacks are here

- Most phishing attacks are still very basic
- Banks want to protect against future styles of attack
- “Man-in-the-Middle” attacks involve a phisher sitting between you and your customer, and modifying data and transactions as they travel across the wire.

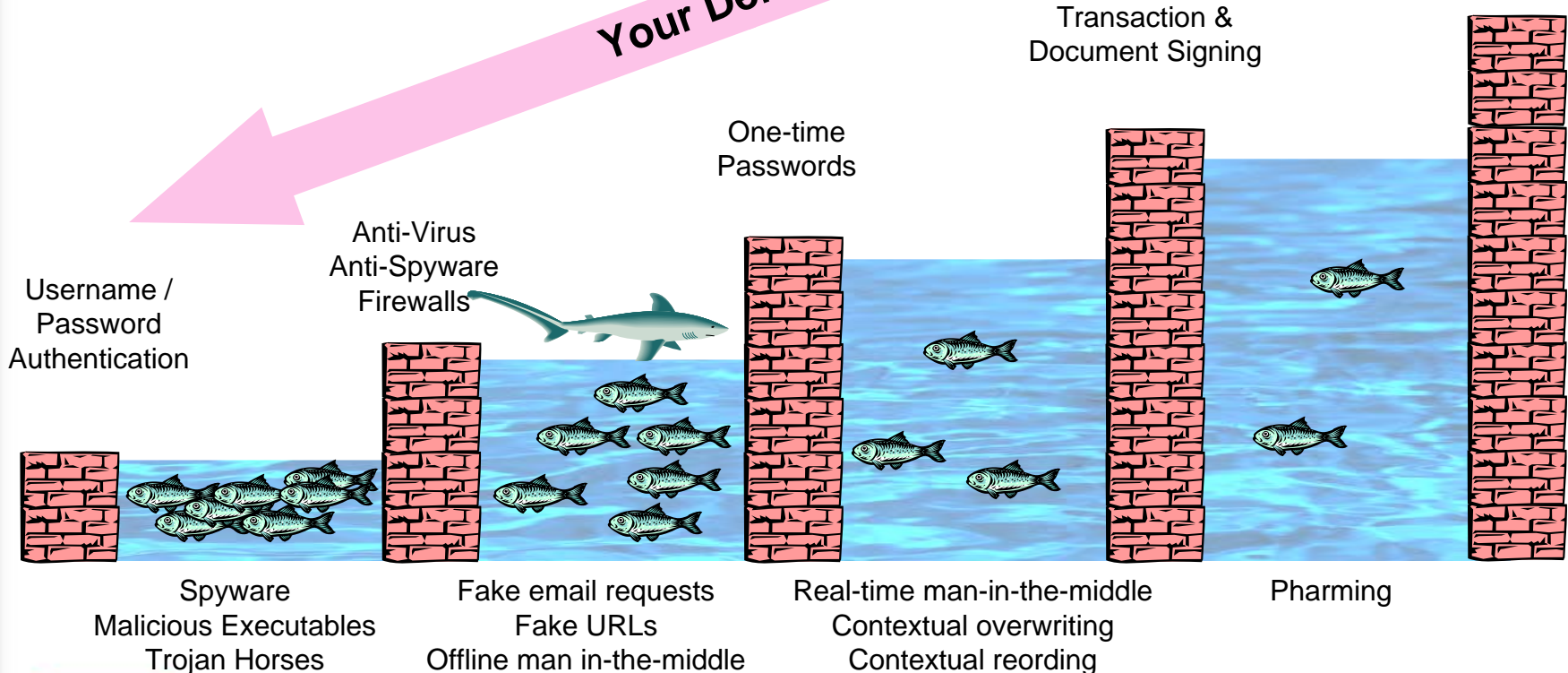


Defenses Against Phishing Techniques

- A variety of tools exist to help protect against phishing attacks
- When implementing a new defense, be sure it moves your customer over the next wall!

Your Defenses

Trusted Computing
Future Technologies



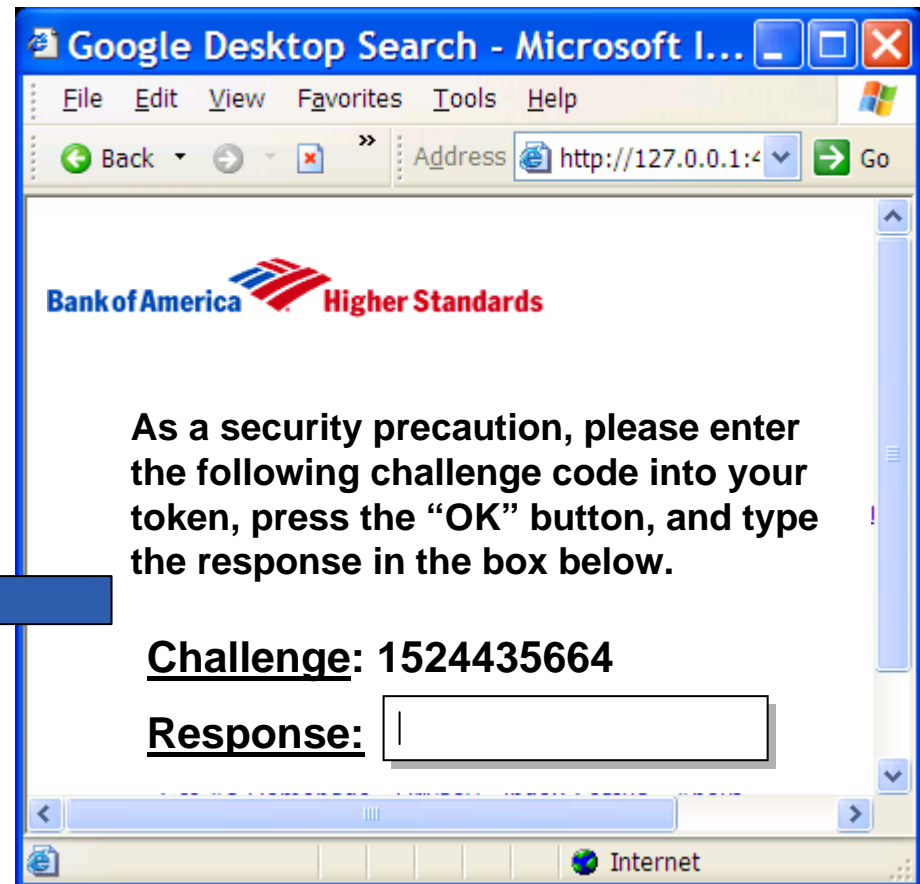
Transaction Signing can also be Vulnerable

- To ease the burden on the user, many banks typically sign just a portion of the account information, like the destination account number.
 - After all, why would a phisher pay any attention to a transaction where they couldn't control the destination account?

OOPS!

**The user just signed the phisher's account number!
The phisher can now authorise a transaction.**

Consider this false page, displayed by the phisher during user's workflow:



Staying Ahead of the Shark

- Anti-virus, Anti-spyware, Firewalls, and One-Time Passwords are good enough to avoid most Phishing attacks today
- Service providers ought to be 2 steps ahead of the shark (so the shark doesn't move into your pond)
- It is impossible to guarantee you won't be the victim of a phishing attack, but proper planning can greatly reduce your exposure
















Determining Your Phishing Defense

- Phishers are dynamic – they will adapt over time
 - There is no silver bullet
- Phishers would rather execute their existing attacks on a new target, then create new attack styles.
- Remember, all MITM phishing attacks *start* with the attacker being able to *hook* the user.
 - A trained or experienced user is a very strong defense
 - Understand your customers to determine their risk levels
- Balance your risk against your defense.













Choosing the Right Solution For You




Your Business Drivers

<i>Web-Based Applications</i>	Ease of Use	Portability	Client-less	Phishing Concerns
SecurID Fob 				
PinPad Token 				
Document Signing 				

Your Business Drivers

<i>Thick Client Applications</i>	Ease of Use	Integration	Phishing Concerns
SecurID Fob 			
PinPad Token 			
Document Signing 			

-  Least desirable
-  Somewhat undesirable
-  Neutral
-  Somewhat desirable
-  Most desirable

How to Stop MITM Attackers

- User training
 - The best defense to real-time man-in-the-middle phishing is to prevent users from getting “hooked” in the first place.
- Disrupt their economy
 - Today, most attacks involve a “hacker” who gets information and sells it online, and a “thief”, who uses that information to execute a fraudulent transaction
 - With time-based one-time-passwords and transaction signatures, the real-time MITM must respond quickly, in an automated fashion, and within a limited time window.
 - This means either the “hacker” and the “thief” must be the same person, or they must be able to react together with extreme efficiency.
- Force the phisher to adapt to new technologies
 - Complicate the ability for the phisher to execute an automated attack
 - Introduce new mechanisms that force the phisher to update their automation capabilities

Creating a Phishing Defense Strategy

1. Understand the phishing risks associated with your customer population(s)
 - Would they supply personal information in response to an unsolicited email request?
 - Would they engage in a financial transaction in response to an unsolicited email request?
 - How familiar are they with financial processes and account-related data?
 - How frequently do they transact, and in what amounts?
 - Is access controlled by one individual or multiple people?
2. Understand the various styles of phishing attacks, and where the state-of-the-art in phishing technology is today
3. Assess your customer's tolerance for various security processes
 - If security processes are too complicated, will customers leave?
 - What will the impact of the security processes be on the customer support org?
4. Balance your risk of exposure against the cost and complexity of the infrastructure



RSA

SECURITY®

Confidence Inspired™