Protecting your System's Data in a Changed Environment

AMERIS BANK

Today's Presenter

Kevin Strickland: Director of Nonprofit and Association Banking

Kevin has over 25 years of banking experience and is responsible for leading Ameris Bank's industry specialization program for water systems, special districts and nonprofit organizations.

Recent Statistics

- Data breaches exposed 4.1 billion records in the first half of 2019. (RiskBased)
- 95% of cybersecurity breaches are caused by human error. (Varonis Cyber Crime Report 2021)
- In 2019, 94% of malware attacks were delivered via email (Verizon's DBIR data)
- Hackers attack every 39 seconds, on average 2,244 times a day. (SF Reporter)
- Since 2017, known attacks on local governments have risen over 50% (GNN)

Understanding Three Common Threats

BUSINESS EMAIL COMPROMISE

Form of cyber crime which use email fraud to attack commercial, government and non-profit organizations

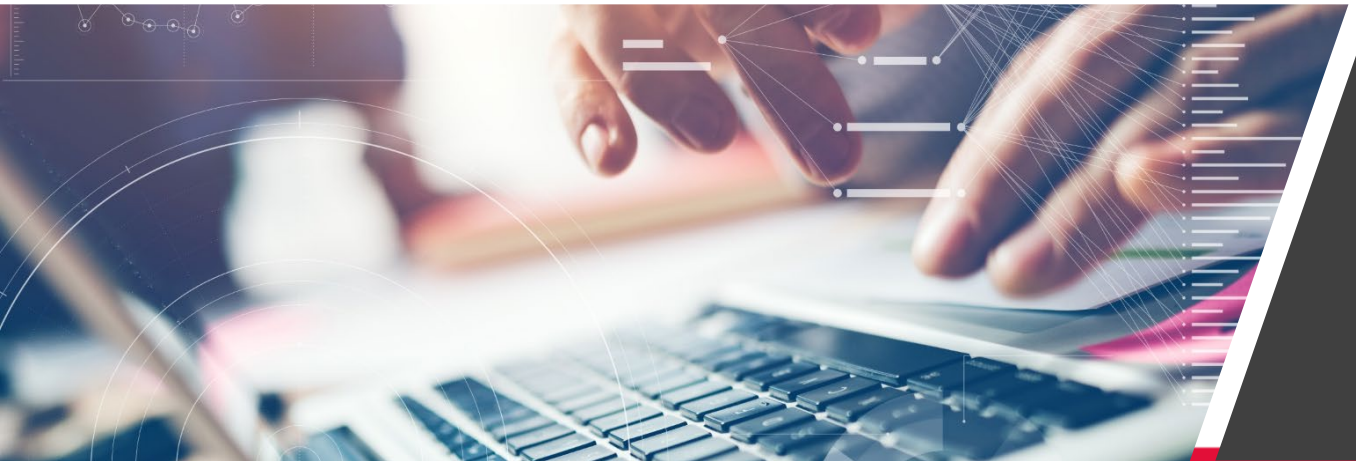
SMISHING

The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal or business information

RANSOM WARE

Threatens to publish your organization's data or perpetually block access to it unless a ransom is paid.

Scheme #1
Business Email Compromise:

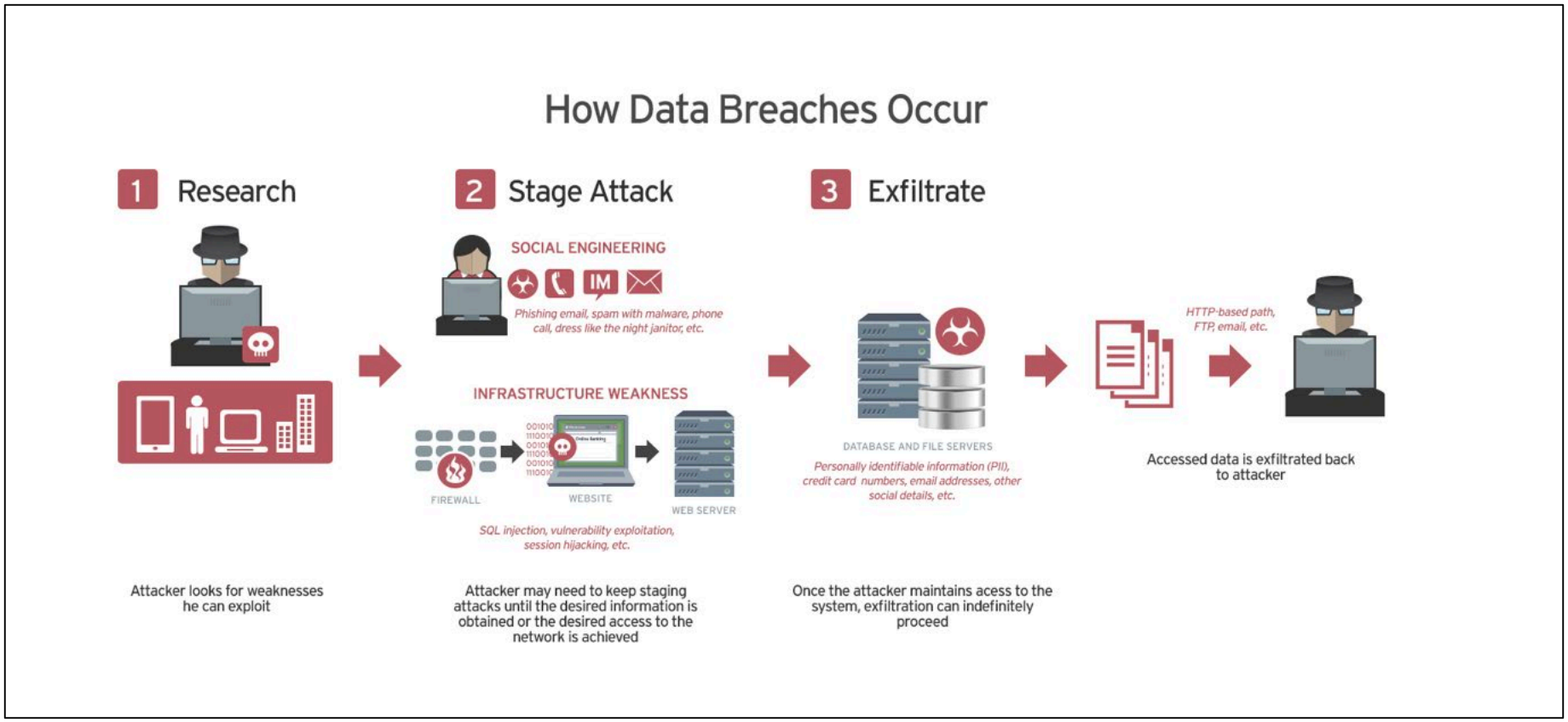


Business Email Compromise (BEC) Statistics

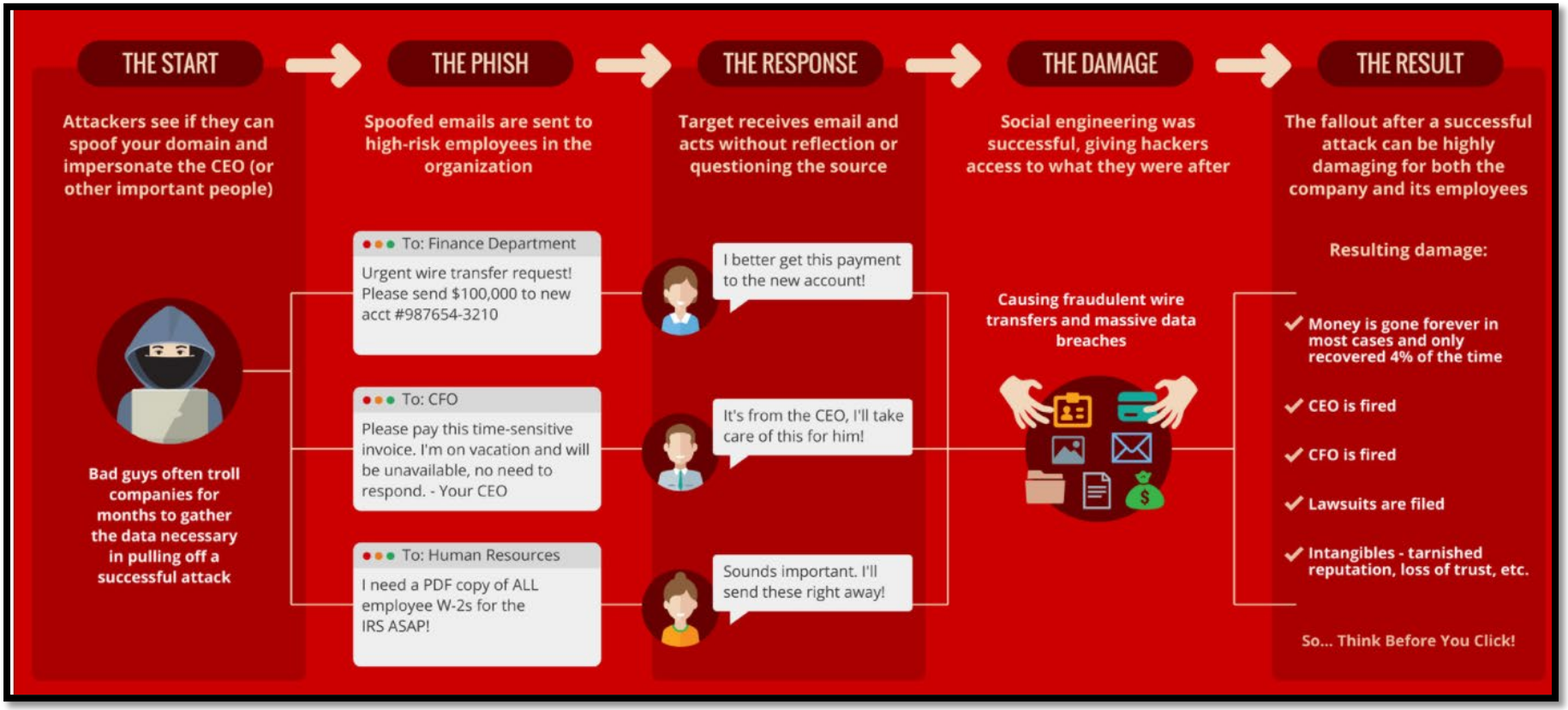
- Between May 2020 and July 2020, there was a 100 percent increase in identified global Business Email Compromise exposed losses (Internet crime complaint center)
- Over the past three years, Business Email Compromise (BEC) schemes have caused at least $5.3 billion in total losses to approximately 24,000 companies around the world (trendmicro)
- During the third quarter of 2020, the median number of business email compromises received per company each week rose by 15% (techrepublic)
- 65% of companies faced business email compromises in 2020 (security Blvd.)

From 2019 to 2020, business email compromise attacks have increased 67% leading to fraud, ransomware, and data breaches

Business Email Compromise: Data Breaches



Business Email Compromise: Spear Phishing



Look at the spelling of the words and names carefully.

Tom.rogers@principlepipe.com

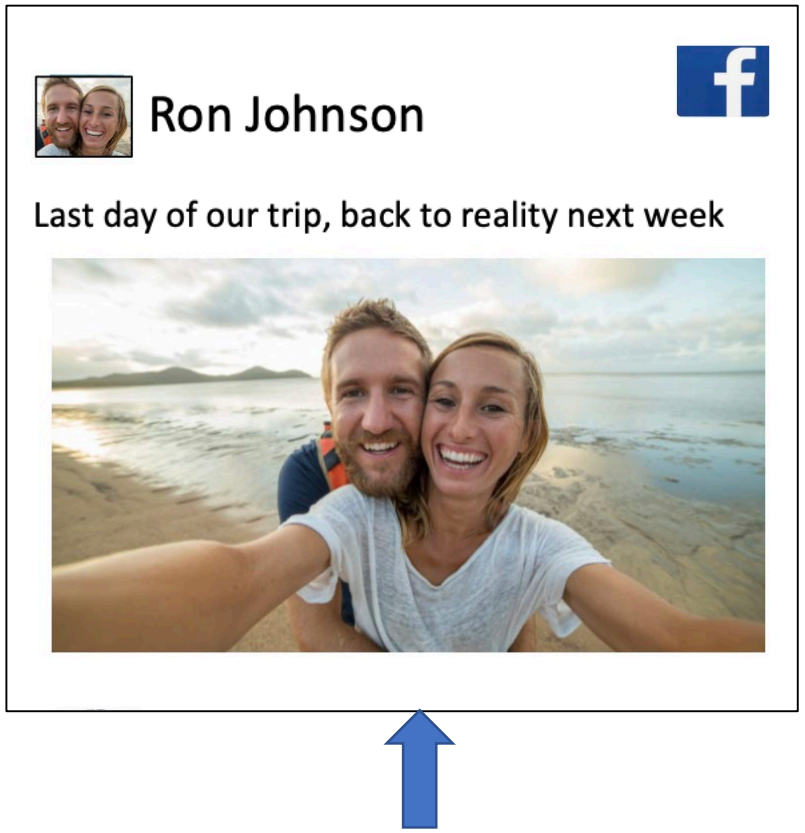
Tom.rogers@principalpipe.com

www.mircosoft.com

Source: KnowBe4 and Trend Micro

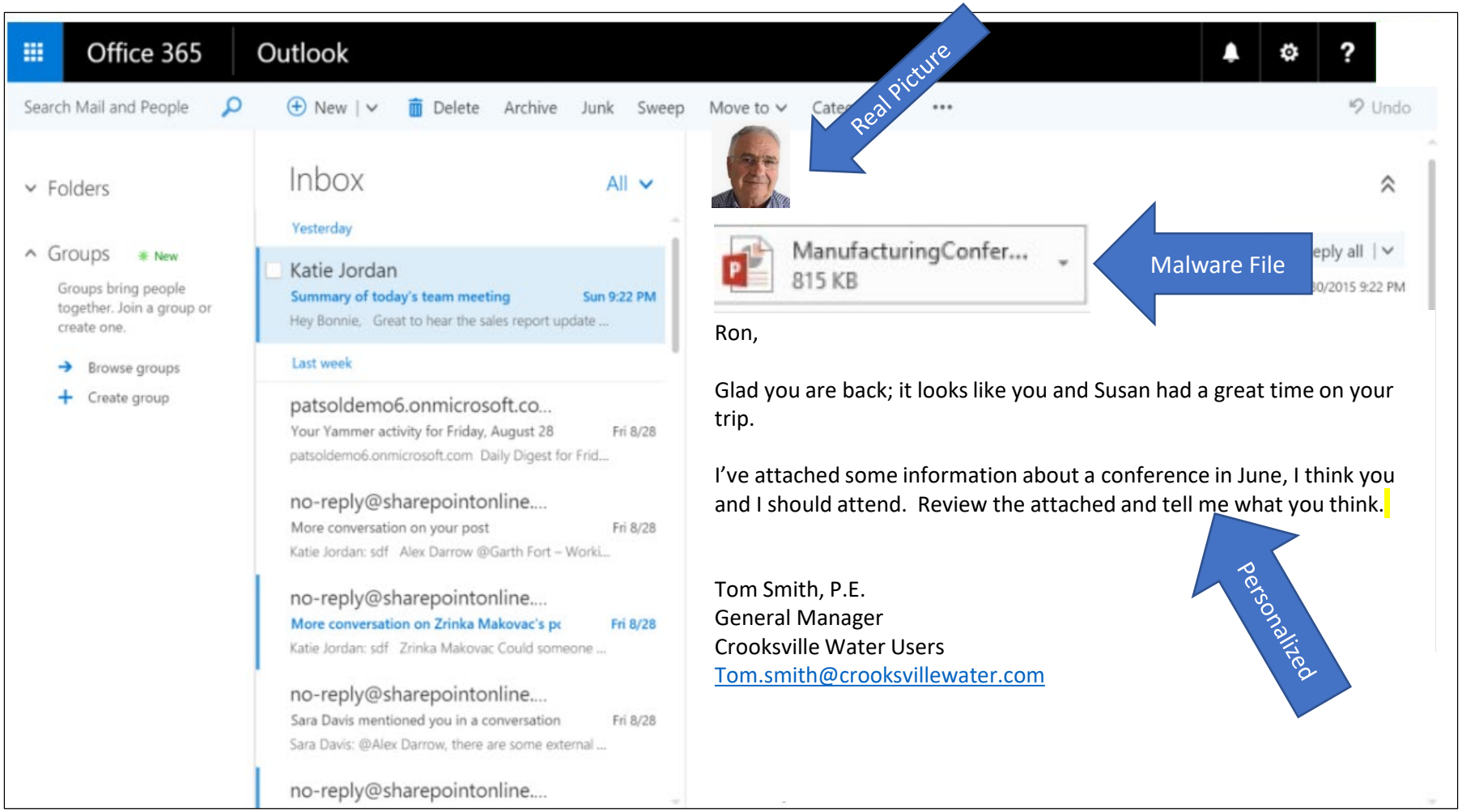
Business Email Compromise: Spear Phishing

- Perpetrators research key individuals and their roles in the company based on information on social media sites, professional associations, company website, etc.
- Crooks look at post for specifics such as job duties/descriptions, hierarchal information and out-of-town travel details
- Fake social media accounts can be created, appearing they are legitimate
- Information about the individual can be used to personalize and legitimize business email attacks.



Fraudsters often review social media sites to legitimize attempted email compromises

Business Email Compromise: Spear Phishing



Sophisticated Attackers Do their Homework

Scheme #2: Smishing

Smishing (Text Fraud)

•Spyware products are available for as little as $30 per month, and some can even be used for free for a limited time. These programs are designed to gather your information to use in identity theft or corporate espionage, or even to spy on you directly by:

- Accessing the camera and microphone in your smartphone
- Recording calls and accesses call logs text messages
- Gaining access to email
- Accessing any files stored on your phone (including contacts)

Smishing: The Warning Signs

1. Unusual data usage spikes.
2. Excessive battery drainage.
3. Apps take a long time to launch.
4. Cell phone restarts for no reason.
5. Background noise.
6. Apps that you don't remember installing.
7. A high number of calls from unrecognized numbers.

Smishing: Ways to Avoid Being a Victim

1. Avoid installing any third-party software on your devices (especially if you use an Android device), only install applications released by trusted developers that have a good amount of positive feedback.

2. Don't store your credit card, banking information or passwords on your smartphone.

3. Never click a reply link or phone number in a message you're not sure about.

4. Visit trusted vendor websites directly (separately from text messages)

5. Don’t click on links asking you to change your password, Instead, type the organization’s URL directly into your browser

Scheme #3: Ransomware

•Ransomware perpetrators carry out more than 4,000 attacks daily.

•On average, organizations pay a ransom of $233,217.

•There’s a 19-day downtime following a ransomware attack.

•95 new ransomware classification families were discovered in 2019 alone.

•Ransomware attacks rose by 388% between Q2 and Q3 of 2020, occurring every 11 seconds.

•The global cost associated with ransomware recovery will exceed $20 billion in 2021

Ransomware

- Fraudster demands ransom to remove the restrictions
- Some forms systematically encrypt files on the system's hard drive.
- Difficult or impossible to decrypt without paying the ransom for the decryption key; some may simply lock the system and display messages to coax the user into paying
- Most Ransomware enters the system through attachments to an email message.

How to Safeguard Your System's Data

- **Be careful with what information you share online or on social media**. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.

- **Don't click on anything in an unsolicited email or text message** asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate

- **Carefully examine the email address, URL, and spelling used in any correspondence**. Scammers use slight differences to trick your eye and gain your trust.

- **Be careful what you download**. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.

For More Information Contact:

Kevin Strickland
Ameris Bank
850-661-3972
Kevin.Strickland@amerisbank.com