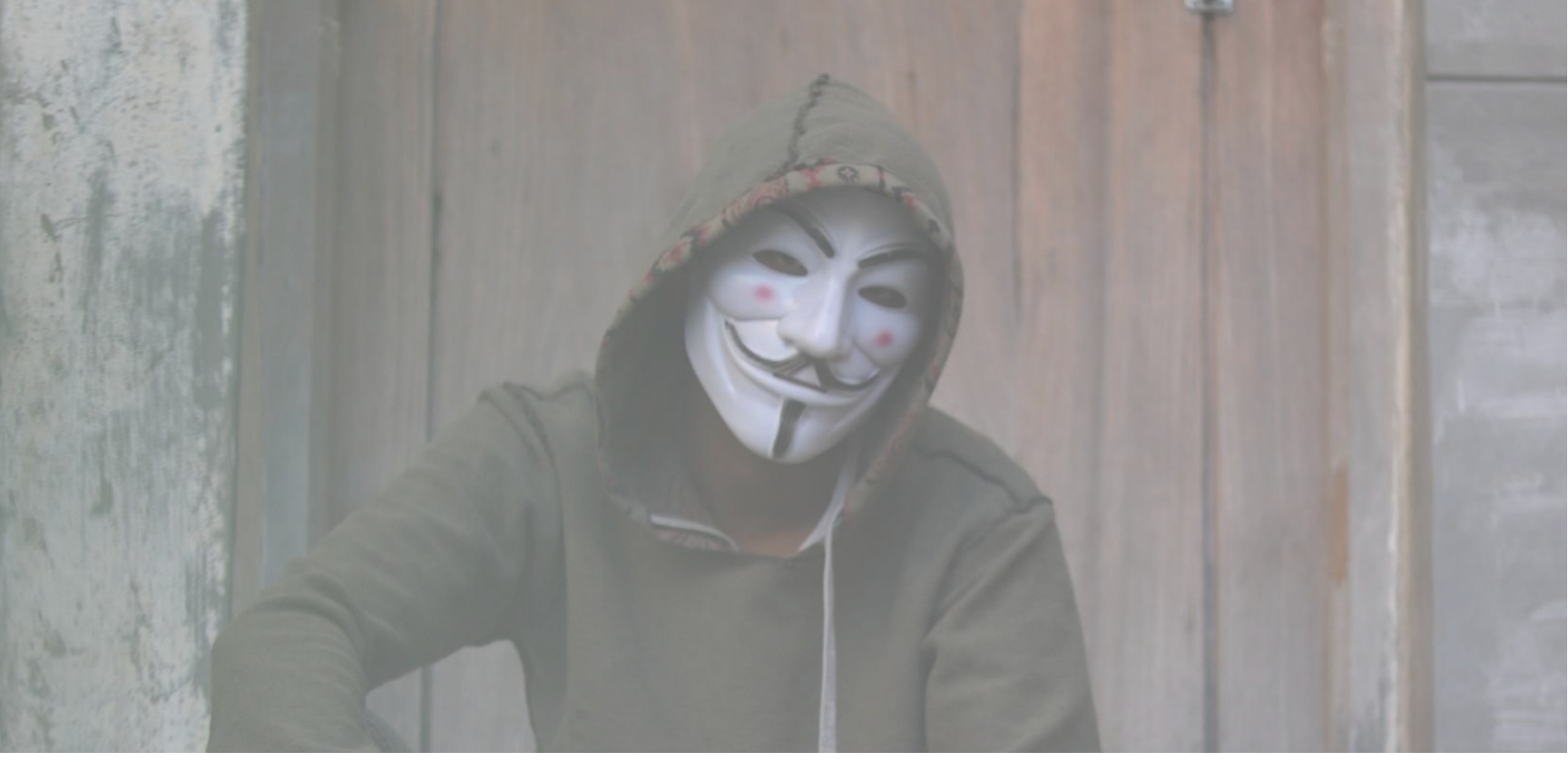
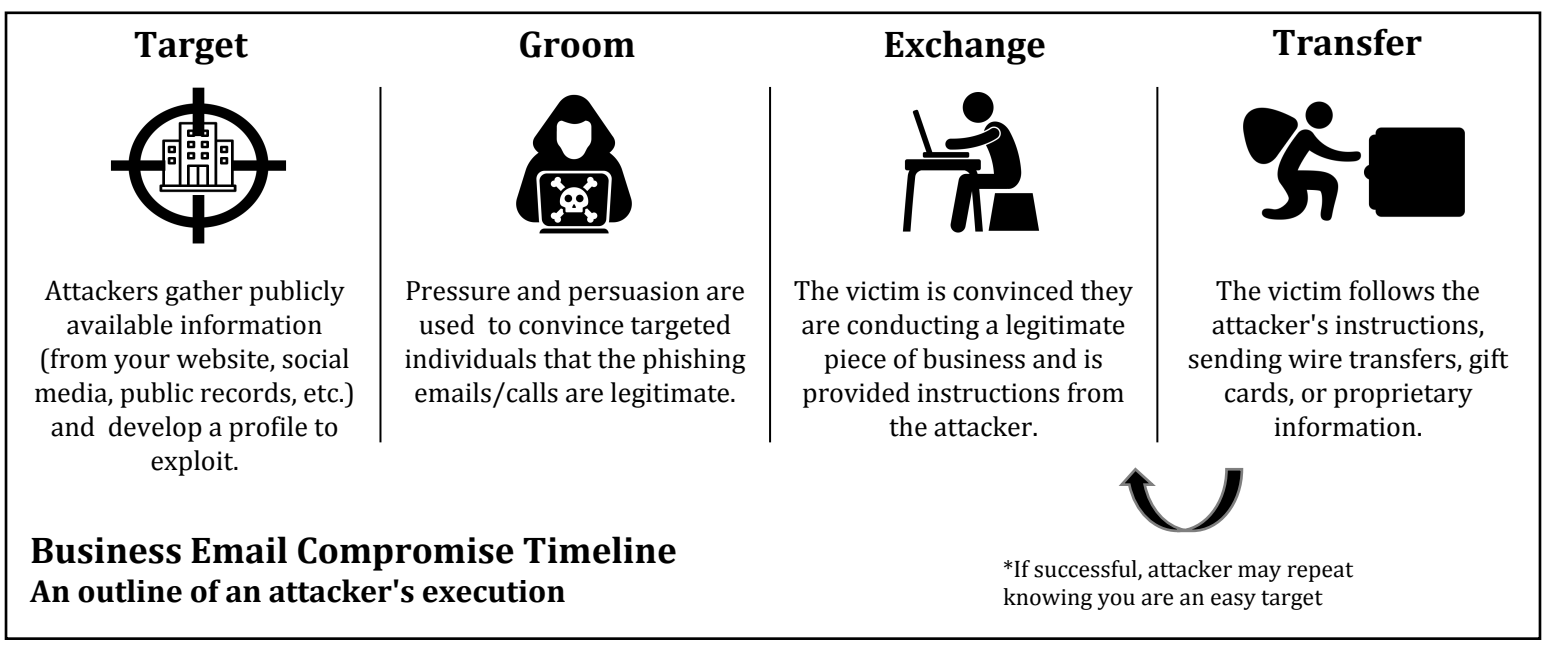


Mitigating Business Email Compromise Risk: Tax Season Security Tips

In 2018, the FBI received over 20,000 complaints of business email compromise, with estimated adjusted losses totaling over $1.2 billion. During their investigations, they found the attacks used to compromise business email have become more evolved.

The storied “Nigerian Prince” scam is no longer the norm, and advanced criminal enterprises are targeting private business, large corporations, local government agencies. The single biggest attack vector in BEC, Phishing, has become far more evolved.

In addition to emails from “CEO@yourcompanyname.scam.com” being opened by untrained end users, a new evolving threat is emails from legitimate (albeit compromised) email addresses. After attackers have compromised a user’s account, they utilize them to elicit trust from their end target. An attacker gaining illicit access to a trusted vendor, a lawyer, or worst case, an internal executive’s email, could be the new launching point for highly targeted spear phishing campaigns. This is a serious evolution of the scam, as traditional methods of detection: checking sending details, spam filters, and firewalls, are of no help.



With Tax Season around the corner, we have identified some of the most prevalent Tax related schemes/attacks that criminal organizations are using today:

IRS Fraud: Various forms of IRS related scams: from receiving fake IRS invoices, notices that you are due a bigger tax refund, or a “court order” because you didn’t pay your taxes.

W2 Fraud: W2 verification or download are the most common attacks in this category, with the “HSA/W2 Confirmation” being a related and equally common scam.

SSN Fraud: Your SSN or EIN has been suspended due to fraudulent activity! In this attack, the scammer will pretend to be some form of law enforcement making sure that you are aware your SSN is connected to criminal enterprises, but that they can help.

While utilizing the above attack vectors, phishers, hackers, and other bad actors use the following three tools to make you and your organization act irrationally and fall for their scams:

In order to maintain your security this tax season, there are several enterprise-level initiatives that can help build better security hygiene:

- **Security Education & Awareness**– Develop informative security education and awareness collateral for circulation throughout your organization in order to homogenize workforce understanding of cyber-security threats and countermeasures applicable to the organization.
- **Phishing Strategy**– Administer phishing awareness trainings and simulations and implement defense measures (e.g. multi-factor authentication, endpoint protection, and quarantine software) to combat external phishing attacks.
- **Offensive Security**– Improve the security of your organization’s most critical assets through external penetration testing and red teaming.
- **Threat Modeling**– Facilitate brainstorming sessions focused on identifying and prioritizing potential threats and vulnerabilities and defining countermeasures to prevent or mitigate associated impact.

If you have any questions regarding attacks and scams this Tax Season or would like additional insight into implementing the cyber-security measures mentioned above, please contact **Michael Morgenstern** (Michael.Morgenstern@dayblink.com) or **Martin Badinelli** (Martin.Badinelli@dayblink.com) at DayBlink Consulting.