KLINGENSTEIN FIELDS
ADVISORS

Q: What is catfishing, and how do I protect myself against it?

A: Catfishing is where a scammer or threat actor (someone who has the potential to impact your cybersecurity) either creates a fake identity or assumes the identity of another person to trick a specific victim. This is in contrast to phishing scams, where the threat actor casts a wider net by sending a more general email message to a broader audience in the hopes of compromising at least one victim.
The two best defenses against both potential catfishing (or phishing) are:

- Don't overshare your information online
- Don't assume that the person with whom you are communicating online is who they say they are. Catfishing is often highly targeted and an be made more convincing by conducting background research on a target. A catfisher can come across as extremely convincing by using information gleaned from social media and other publicly available information.

Q: Once you are compromised, are you more likely to continue to be compromised going forward?

A: Unfortunately, yes. Once your personal data is out there, there’s no way to put the genie back in the bottle. Breached data can, and most likely will, be copied, archived, repackaged, and sold on the dark web for as long as it’s considered valuable. And, as in the case of millions of Social Security Numbers, that value could continue beyond your lifetime. The same goes for organizations: statistics suggest that some 80 percent of ransomware victims are going to be attacked again.

Q: Is using Russian-owned virus software like Kaspersky unwise?

A: While Kaspersky anti-virus software is generally well-reviewed and a popular option for consumers, the State Department banned its products from all government departments in 2017 due to alleged ties to the Russian government (since these allegations, Kaspersky has moved its data processing centers to Switzerland, opened Transparency Centers, and passed a Service Organization Control 2 audit, which "provides detailed information and assurance about a service organization's security, availability, processing integrity, confidentiality, and/or privacy controls, based on their compliance with the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria). No concrete proof of foul play has come to light, and Kaspersky products are still widely used throughout the world, but rumors persist. If you're dealing with especially sensitive information, you may want to steer clear and err on the side of caution, with the caveat, however, that other security software packages may come with similar concerns as to data sharing.

Q: In my family, we all tend to share devices, including the kids. How worried should I be about that?

A: The more people using a device, the more avenues there are for it to be compromised. Every user, every app, every incoming or outgoing message increase a device's (and by proxy your) attackable surface. If getting your kids their own devices (which comes with its own set of security and privacy concerns) sounds expensive, consider the potential cost of your financial, medical, or professional data being compromised. Additionally, what if your shared device is compromised and threat actors use information gleaned from the data it stores to access your company's networks, creating legal, regulatory, and financial consequences?

Q: I have all of the up-to-date security tools on my devices, I should be ok right?

A: While having more protection is always a plus, it doesn't mean that you're fully protected, any more than wearing a seatbelt and having air bags can protect you from crashing a car. "Safer" is very different from "safe." Keeping the security programs on your devices up-to-date is a great step, but it shouldn't give you the idea that you're 100% secure. You can still be compromised by a reused or discovered password, a mistaken click, or unsafe activity from anyone else using your device.

Q: Do most cloud backup programs detect ransomware on files as they prepare to back up?

A: Some backup programs may run security scans on files on their servers, but ransomware has become a multi-billion-dollar industry by being clever and hard to detect. Regular backups can help stop a ransomware attack in its tracks, but bear in mind that cloud-based products and services also come with their own set of security concerns.

Q: What are your perspectives on voice recognition?

A: In the era of deepfake technology, it's becoming increasingly easy to imitate a voice, especially if there's a lot of existing data out there. For that reason, voice recognition can be vulnerable to attacks using cloned voice samples that are created using online voice clips from platforms such as YouTube, TikTok, and other social media. For that reason, we would still recommend other security measures, such as two-factor authentication.

Q: Do you have a set of specific recommendations for security providers for long password managers, two-factor authenticators, life lock type programs that check credit card use abnormalities, identity theft security firms, and credit evaluation abnormalities.

A: We generally don't recommend specific products or services because there are many very good ones (and several that aren't so good). When shopping for identity theft products, services, etc. always read reviews and pay particular attention to negative reviews. There are some organizations that provide insight that you may find helpful:

Consumer Federation of America
https://idtheftinfo.org/shopping-for-id-theft-services

Consumer Reports
https://www.consumerreports.org/search/?query=identity+theft+products+and+services